

# **NAVAL POSTGRADUATE SCHOOL**

## **Monterey, California**



## **THESIS**

### **IMPLEMENTING THE NAVAL POSTGRADUATE SCHOOL'S SECURITY POLICY USING WINDOWS 2000**

by

David R. McKinley

September 2001

Thesis Advisor:  
Associate Advisors:

Paul Clark  
William Haga  
Doug Brinkley

**Approved for public release; distribution is unlimited.**

## Report Documentation Page

<b>Report Date</b> 30 Sep 2001	<b>Report Type</b> N/A	<b>Dates Covered (from... to)</b> -
<b>Title and Subtitle</b> Implementing the Naval Postgraduate Schools Security Policy Using Windows 2000	<b>Contract Number</b>	
	<b>Grant Number</b>	
	<b>Program Element Number</b>	
<b>Author(s)</b> David R McKinley	<b>Project Number</b>	
	<b>Task Number</b>	
	<b>Work Unit Number</b>	
<b>Performing Organization Name(s) and Address(es)</b> Research Office Naval Postgraduate School Monterey, Ca 93943-5138	<b>Performing Organization Report Number</b>	
<b>Sponsoring/Monitoring Agency Name(s) and Address(es)</b>	<b>Sponsor/Monitor's Acronym(s)</b>	
	<b>Sponsor/Monitor's Report Number(s)</b>	
<b>Distribution/Availability Statement</b> Approved for public release, distribution unlimited		
<b>Supplementary Notes</b>		
<b>Abstract</b>		
<b>Subject Terms</b>		
<b>Report Classification</b> unclassified	<b>Classification of this page</b> unclassified	
<b>Classification of Abstract</b> unclassified	<b>Limitation of Abstract</b> UU	
<b>Number of Pages</b> 317		

<b>REPORT DOCUMENTATION PAGE</b>			<i>Form Approved</i> <i>OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
<b>1. AGENCY USE ONLY (Leave blank)</b>		<b>2. REPORT DATE</b> September 2001	<b>3. REPORT TYPE AND DATES COVERED</b> Master's Thesis	
<b>4. TITLE AND SUBTITLE:</b> Implementing the Naval Postgraduate School's Security Policy Using Windows 2000			<b>5. FUNDING NUMBERS</b>	
<b>6. AUTHOR(S)</b> David R McKinley				
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> Naval Postgraduate School Monterey, CA 93943-5000			<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>	
<b>9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> N/A			<b>10. SPONSORING / MONITORING AGENCY REPORT NUMBER</b>	
<b>11. SUPPLEMENTARY NOTES</b> The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
<b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b> Approved for public release; distribution is unlimited.			<b>12b. DISTRIBUTION CODE</b>	
<p>When the Naval Postgraduate School (NPS) fully migrates to Microsoft Windows 2000 as the primary operating system on desktop PCs and servers, security configuration will be a major concern. Windows 2000 provides a consolidated tool set as a means to securely configure these systems. It also provides a pre-configured list of security templates that may be applied when initially configuring different types of systems. The purpose of this thesis is to provide: (1) brief overview of the Microsoft Windows 2000 security architecture, (2) a description of the Windows 2000 Security Configuration Tool Kit and how to configure security settings, (3) a discussion on security policy and how it effects security configurations, (4) recommendations on how to translate the Naval Postgraduate School's Security Policy into Windows 2000 security settings, and (5) a pre-configured, recommended security template for all students attending NPS.</p>				
<b>14. SUBJECT TERMS</b> Windows 2000, Computer Security, Operating System Security			<b>15. NUMBER OF PAGES</b>	
			<b>16. PRICE CODE</b>	
<b>17. SECURITY CLASSIFICATION OF REPORT</b> Unclassified	<b>18. SECURITY CLASSIFICATION OF THIS PAGE</b> Unclassified	<b>19. SECURITY CLASSIFICATION OF ABSTRACT</b> Unclassified	<b>20. LIMITATION OF ABSTRACT</b> UL	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**IMPLEMENTING THE NAVAL POSTGRADUATE SCHOOL'S SECURITY  
POLICY USING WINDOWS 2000**

David R. McKinley  
Lieutenant Colonel, United States Marine Corps  
B.A. Indiana University, 1983  
M.B.A. New Hampshire College, 1995

Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT**

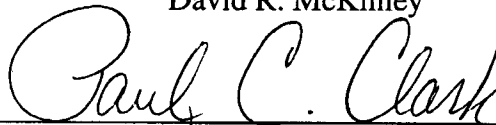
from the

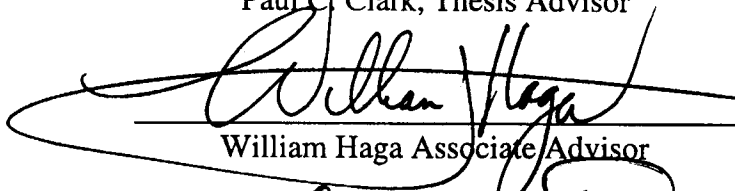
**NAVAL POSTGRADUATE SCHOOL  
September 2001**

Author:


  
David R. McKinley

Approved by:

  
Paul C. Clark, Thesis Advisor

  
William Haga Associate Advisor

  
Doug Brinkley, Associate Advisor

  
Chris Eagle, Chairman  
Information Systems Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

When the Naval Postgraduate School (NPS) fully migrates to Microsoft Windows 2000 as the primary operating system on desktop PCs and servers, security configuration will be a major concern. Windows 2000 provides a consolidated tool set as a means to securely configure these systems. It also provides a pre-configured list of security templates that may be applied when initially configuring different types of systems. The purpose of this thesis is to provide: (1) brief overview of the Microsoft Windows 2000 security architecture, (2) a description of the Windows 2000 Security Configuration Tool Kit and how to configure security settings, (3) a discussion on security policy and how it effects security configurations, (4) recommendations on how to translate the Naval Postgraduate School's Security Policy into Windows 2000 security settings, and (5) recommendations on a pre-configured, security template for all students attending NPS.

THIS PAGE INTENTIONALLY LEFT BLANK



## TABLE OF CONTENTS

<b>I. INTRODUCTION TO WINDOWS 2000 SECURITY ARCHITECTURE.....</b>	<b>1</b>
<b>A. INTRODUCTION .....</b>	<b>1</b>
1. Problem .....	1
2. Solutions Offered by this Thesis .....	1
3. Consequences if Problem is Not Solved.....	1
<b>B. THE NT LEGACY .....</b>	<b>2</b>
<b>C. INTRODUCTION TO WINDOWS 2000 SECURITY .....</b>	<b>5</b>
<b>D. ACTIVE DIRECTORIES .....</b>	<b>6</b>
<b>E. AUTHENTICATION SERVICES AND KERBEROS.....</b>	<b>7</b>
<b>F. CERTIFICATE SERVER .....</b>	<b>9</b>
<b>G. ENCRYPTED FILE SERVICE.....</b>	<b>9</b>
<b>H. IPSEC .....</b>	<b>10</b>
<b>I. SUMMARY .....</b>	<b>10</b>
<b>II. THE NAVAL POSTGRADUATE SCHOOL’S SECURITY POLICY.....</b>	<b>13</b>
<b>A. INTRODUCTION .....</b>	<b>13</b>
<b>B. DEFINING SECURITY POLICY .....</b>	<b>13</b>
<b>C. EFFECTIVE SECURITY POLICY .....</b>	<b>15</b>
<b>D. CHAPTER SUMMARY .....</b>	<b>17</b>
<b>III. ATTACK METHODOLOGIES AND PREVENTATIVE MEASURES.....</b>	<b>19</b>
<b>A. INTRODUCTION .....</b>	<b>19</b>
<b>B. THE SECURITY RISK FROM INSIDERS AND MITIGATION</b>	
<b>TECHNIQUES .....</b>	<b>19</b>
1. Attack Methodology .....	19
2. Scanning.....	20
3. Enumeration .....	22
4. Gaining Access and Escalating Privileges.....	25
<b>C. SUMMARY.....</b>	<b>28</b>
<b>IV. RECOMMENDATIONS FOR THE SECURITY TEMPLATE AND FINAL</b>	
<b>THOUGHTS.....</b>	<b>29</b>
<b>A. INTRODUCTION .....</b>	<b>29</b>
<b>B. SECURITY SETTINGS USING TEMPLATES .....</b>	<b>29</b>
1. Introduction to Security Templates.....	29
2. Security Options.....	30
3. Password Policies.....	32
4. Account Lockout Policies.....	32
5. Audit Policy.....	32
6. Audit Log Settings.....	33
7. User Rights.....	33
<b>C. AREAS FOR FURTHER STUDY AND CONSIDERATION .....</b>	<b>34</b>
<b>D. FINAL THOUGHTS.....</b>	<b>35</b>

<b>LIST OF REFERENCES .....</b>	<b>37</b>
<b>APPENDIX A: WINDOWS SECURITY TOOL SET .....</b>	<b>39</b>
<b>A. INTRODUCTION .....</b>	<b>39</b>
<b>B. SECURITY POLICY .....</b>	<b>39</b>
<b>C. WINDOWS 2000 WORKSTATIONS AND SERVERS .....</b>	<b>40</b>
1. Windows 2000 Professional and Member Servers .....	40
2. Windows 2000 Domain Controllers .....	42
<b>D. WINDOWS SECURITY CONFIGURATION AND ANALYSIS TOOL .....</b>	<b>43</b>
<b>E. DEFAULT SECURITY TEMPLATES .....</b>	<b>44</b>
1. Conpat.inf .....	45
2. Securews.inf and Securedc.inf .....	46
3. Hisecdc.inf and Hisecws.inf .....	47
<b>F. ANALYZING AND CONFIGURING THE LOCAL MACHINE .....</b>	<b>47</b>
<b>G. SECURITY CONFIGURATION AND ANALYSIS AREAS .....</b>	<b>49</b>
1. Account Policies .....	49
2. Kerberos Policy .....	50
3. Local Policies .....	51
4. Audit Policy .....	53
5. User Rights .....	54
6. Event Log .....	55
7. Restricted Groups .....	56
8. System Services .....	56
9. Registry .....	56
10. File Systems .....	56
11. Encrypted File System .....	56
12. Internet Protocol Security Policies on Local Computer .....	57
<b>H. SUMMARY OF SECURITY TOOL SET .....</b>	<b>57</b>
<b>APPENDIX B. SECURITY SETTINGS BY POLICY .....</b>	<b>59</b>
<b>A. ENABLED .....</b>	<b>59</b>
<b>B. DISABLED .....</b>	<b>59</b>
<b>C. NOT DEFINED .....</b>	<b>60</b>
<b>D. NOT GRANTED .....</b>	<b>60</b>
<b>E. COMPARISON OF GROUP CAPABILITIES .....</b>	<b>61</b>
<b>APPENDIX C: RECOMMENDED NPS SECURITY POLICY .....</b>	<b>63</b>
<b>A. FORWARD .....</b>	<b>63</b>
<b>B. INTRODUCTION .....</b>	<b>63</b>
<b>C. COMPUTER SECURITY POLICY .....</b>	<b>65</b>
1. Purpose .....	65
2. Policy Scope .....	65
3. Policy Statements .....	65
4. Policy Administration .....	67
5. Electronic Mail Privacy .....	67
<b>ANNEX A - TERMS AND DEFINITIONS .....</b>	<b>67</b>
<b>ANNEX B - PASSWORD MANAGEMENT .....</b>	<b>68</b>

1. Password Selection .....	68
2. Password Handling .....	69
ANNEX C - DISASTER RECOVERY.....	70
1. Data Backup.....	70
2. Contingency Planning.....	70
ANNEX D - PERSONNEL SECURITY AND SECURITY AWARENESS..	70
1. Permanent Personnel and Student Requirements .....	70
ANNEX E - COMPUTER SECURITY RULES, REGULATIONS, AND LAWS .....	71
ANNEX F - FILING COMPLAINTS ABOUT COMPUTER GENERATED HARASSMENT OR DISCRIMINATION .....	72
APPENDIX G - COMPUTER SECURITY POLICY SUMMARY STATEMENT.....	72
APPENDIX D: GROUP POLICY SETTINGS.....	75
INTRODUCTION.....	75
SUMMARY TABLE OF POLICY SETTINGS.....	76
COMPUTER CONFIGURATION.....	96
SOFTWARE SETTINGS.....	96
Software Installation .....	96
WINDOWS SETTINGS .....	96
Scripts (Startup / Shutdown).....	96
Security Settings .....	96
<i>Account Policies</i> .....	96
<i>Local Policies</i> .....	102
<i>Event Logs</i> .....	132
<i>Restricted Groups</i> .....	137
<i>System Services</i> .....	137
<i>Registry</i> .....	137
<i>File System</i> .....	137
<i>Public Key Policies</i> .....	137
<i>IP Security Policies on Active Directory</i> .....	137
ADMINISTRATIVE TEMPLATES .....	137
Windows Components .....	137
<i>Net Meeting</i> .....	137
<i>Internet Explorer</i> .....	137
<i>Task Scheduler</i> .....	140
<i>Windows Installer</i> .....	143
System.....	148
<i>Logon</i> 152	
<i>Disk Quotas</i> .....	158
<i>DNS Client</i> .....	161
<i>Group Policies</i> .....	162
<i>Windows File Protection</i> .....	172
Network.....	173

<i>Offline Files</i> .....	173
<i>Network and Dial-up Connections</i> .....	181
Printers.....	181
<b>USER CONFIGURATION</b> .....	188
<b>SOFTWARE SETTINGS</b> .....	188
Software installation .....	188
<b>WINDOWS SETTINGS</b> .....	188
IE maintenance.....	188
<i>Browser user interface</i> .....	188
<i>Connection</i> .....	188
<i>URLs</i> .....	188
<i>Security</i> .....	188
<i>Programs</i> .....	188
Scripts.....	188
Security Settings .....	189
<i>Public key policies</i> .....	189
<i>Remote Installation Service</i> .....	189
Folder Redirection.....	189
<i>Application Data</i> .....	189
<i>Desktop</i> .....	189
<i>My Documents</i> .....	189
<i>Start Menu</i> .....	189
<b>ADMINISTRATIVE TEMPLATES</b> .....	189
Windows Components .....	189
<i>Netmeeting</i> .....	189
<i>Internet Explorer</i> .....	193
<i>Windows Explorer</i> .....	227
<i>Microsoft Management Console</i> .....	235
<i>Task Scheduler</i> .....	241
<i>Windows Installer</i> .....	244
Start Menu and Taskbar .....	246
Desktop.....	253
<i>Active desktop</i> .....	256
<i>Active directory</i> .....	260
Control panel .....	261
<i>Add/Remove programs</i> .....	262
<i>Display</i> .....	266
<i>Regional options</i> .....	270
Network.....	270
<i>Offline files</i> .....	270
<i>Network and dialup connections</i> .....	276
System.....	285
<i>Logon/Logoff</i> .....	289
<i>Group Policy</i> .....	294
<b>INITIAL DISTRIBUTION LIST</b> .....	299

## **LIST OF FIGURES**

Figure 3.1 The Anatomy of an Attack (from Scambray, 2001) .....	20
---	----

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF TABLES

Table 4.1 Security Options.....	32
Table 4.2 Password Policy Settings .....	32
Table 4.3 Account Lockout Settings .....	32
Table 4.4 Audit Policy Settings.....	33
Table 4.5 User Rights Assignment.....	34

THIS PAGE INTENTIONALLY LEFT BLANK



## **ACKNOWLEDGMENTS**

First, I would like to thank the Lord for giving me peace and strength through this process, then I would like to thank my supportive family: Amy, Megan, Brendan, thank you for your patience. Thank you to DISA, N64/SPAWAR, and Dr. Cynthia Irvine for your financial assistance in supporting my Windows 2000 training requirements. Professionally, I would like to thank my advisors, Mr. Paul Clark, Dr. William Haga, and Mr. Doug Brinkley.

THIS PAGE INTENTIONALLY LEFT BLANK

# **I. INTRODUCTION TO WINDOWS 2000 SECURITY ARCHITECTURE**

## **A. INTRODUCTION**

### **1. Problem**

In order to properly configure the security of a workstation that resides on a network, there should be enterprise level guidance in order that all the systems have a similar configuration. Within the confines of the NPS network, this configuration guidance is currently not available. Administrators currently configure the security of Windows 2000 without central guidance from the network security officer. Therefore, this thesis is focused on addressing two problems. First, it will give recommendations on a workable enterprise level security policy that can be adapted school wide, and second, it will give recommendations on how to configure a security template (new in Windows 2000) to give administrators a way to enhance security against insider attacks. This template is portable to all workstations on the network. There is currently no configuration guidance for Windows 2000 from the National Security Agency or the Space and Naval Warfare Systems Command. This lack of central guidance could possibly lead to severe problems with security.

### **2. Solutions Offered by this Thesis**

This thesis will provide several solutions to the problems listed above. First, after an overview of the Windows 2000 security features are discussed in Chapter I, this thesis will provide guidance on writing an effective security policy. Second, it will make recommendations on how to translate the Naval Postgraduate School Security Policy into Windows 2000 security settings. Third, it will provide a security template, configured for Windows 2000 Professional, for all students attending NPS. The security template will provide a portable, flexible, enterprise wide set of security settings to any Windows 2000 computer on the NPS network.

### **3. Consequences if Problem is Not Solved**

If NPS fails to implement a security policy that is both enforceable and is of the proper scope, then it is difficult to deploy Windows 2000 and leverage its full

functionality. Additionally, the ability to design a user security template makes the security management of Windows 2000 considerably easier than Windows NT. Therefore, if the deployment of Windows 2000 at the Naval Postgraduate School is conducted in the same manner as Windows NT and the administrators are allowed to configure security settings without the enterprise-wide guidance on security template development, then there is a serious risk to the interoperability of the operating system with other Windows 2000 machines and the potential for security breaches is much higher.

## **B. THE NT LEGACY**

In 1997, the Department of the Navy and the United States Marine Corps agreed to implement IT-21 as their information architecture of the future. The plan called for Microsoft Windows NT 4.0 and future upgrades as the operating and networking system to be used by all Navy commands (United States Naval Message, 1997). Although there is not yet a formal requirement for the Navy to upgrade to the Windows 2000 series operating system, Windows 2000 professional (the workstation upgrade to Windows NT Workstation 4.0) has been deployed on selective desktops throughout the Naval Postgraduate School.

Currently within the Naval Postgraduate School (NPS), the security settings for Windows NT and Windows 2000 Professional are configured based on, but not strictly adhering to, the Space and Naval Warfare Systems Command's (SPAWAR) *Secure Windows NT Installation and Configuration Guide* (SPAWAR, 1998). The SPAWAR guide consists of installation and configuration procedures for securing the Windows NT 4.0 operating system (SPAWAR, 1998).. This document complements the guidance put forth in the National Security Agency's *Guide to Securing Windows NT Networks* (National Security Agency, 2000). These procedures walk the administrator through a step-by-step process that will lead to a C2-level of security.

C2 is a reference to a level of security outlined in the *Department of Defense Trusted Computer System Evaluation Criteria* (National Computer Security Center, 1985). The key component to C2 security is Discretionary Access Control where all

files, devices, processes, etc. are treated as objects, and the object's owner can control all access to their objects.

This chapter will begin by addressing some of the shortfalls of the Windows NT 4.0 operating system and then, it will look at some of the security features of the Windows 2000 operating system. There is a marked improvement in the design of Windows 2000 and functionality of the built-in security features, but due to the limited scope of this thesis only the most important features will be covered.

NT 4.0 was designed as a networking operating system for the enterprise. It had gone through two previous versions, NT 3.50 and NT 3.51. These versions met with limited success because of numerous security and compatibility problems (Manasi, 1999). Windows NT 4.0 was designed to be more secure, scalable, and compatible. It used the well-defined client/server architecture to provide the ability to logon to the network from one workstation and have the user's profile and files available from a central server. It also provided fairly secure central administration and configuration. Although the software engineers at Microsoft laid a solid foundation in their security design of NT 4.0 they have published 7 service packs (patches to fix security holes and bugs in the operability of the software) for the operating system. Therefore, although NT 4.0 was designed with security in mind, there are still security fixes that need to be periodically applied, and it will continue to have security vulnerabilities in the foreseeable future. The security problems in NT 4.0 exist because it is easy to use, designed to be open to other applications, possesses programming flaws, and relatively easy to administer. It is important to note, however, a skilled administrator can secure a Windows NT network with a comfortable level of confidence if he/she follows all the best practices and ensures all the latest security patches are applied.

When the networking software found its niche in the enterprise environment, both administrators and others discovered numerous inadequacies. For example, many of NT's security holes stemmed from backward compatibility with LAN Manager, an IBM add-on product that was used to provide basic authentication across the network. These holes are caused by the division of the NT logon password into two, seven character strings. This is a huge security concern that still plagues NT 4.0 because it makes brute force

password attacks practical with tools such as L0phtcrack. Another problem stems from the delegation of assigning administrative privileges. It is an all or nothing proposition with NT. A user with administrator privileges under Windows NT4.0 can do virtually anything he/she wishes to do on the network. No granularity exists in assigning specific functions to specific users or administrators. For instance, you can't give Help desk personnel the right to reset passwords on user accounts without giving them full administrative privileges.

Another difficulty with NT 4.0 is it does not scale well for large organizations because it is limited to domains of 20,000 users or less and the Primary Domain Controllers (PDCs) and Backup Domain Controllers (BDCs) used one-to-many replication. This one-to-many replication model means that the PDC is the only domain controller that has a read and write copy of the domain database. All other domain controllers are BDCs. The PDC replicates all changes in the domain database to the BDCs. With Windows NT 4.0, the PDC must always be accessible for changes to be made to user accounts, groups, and so forth. If the PDC server is down or if there are network disconnects, the directory is unavailable for changes. (Manasi, 1999)

It was also designed with a flat name space that consisted of User, Global group, Local group and computer accounts. This flat name space was not hierarchical; everything was on the same level. There is no built-in ability to inherit rights and permissions because there is not a higher level. With Windows NT, updating accounts can only be conducted at the PDC, limiting the flexibility of the administrator in dealing with account management.

NT 4.0 is still the standard used throughout the Department of the Navy and will continue to be used in the foreseeable future. System administrators and IT managers can stay abreast of NT 4.0 security vulnerabilities through several online resources such as Ntbugtraq.com or CERT.org, and as long as systems are kept up to date, NT 4.0 can be made to be a fairly secure system.

### **C. INTRODUCTION TO WINDOWS 2000 SECURITY**

Microsoft designed Win2K with several goals in mind to address NT's shortcomings. First, the company designed it for an overall improvement in security. Microsoft added Kerberos 5 network authentication to address vulnerabilities with NT LAN Manager (NTLM) authentication. Win2K's implementation of Public Key Infrastructure (PKI) can also be used to eliminate the risks inherent to passwords, and smart cards to mitigate the risks of private keys. Physical access to hard disks is a known security problem, and especially with the theft of laptops; information is easily accessible once the media is in hand. In response, Microsoft has developed a new Encrypting File System (EFS) in Win2K. The hierarchical directory structure and Group Policy security settings that Windows 2000 (Win2K) provides gives administrators the ability to manage user accounts and system configuration that scale well.

Second, Win2K relies heavily on industry standards and protocols. Win2K uses standards such as Lightweight Directory Access Protocol (LDAP), Kerberos, Public Key Cryptography Standards (PKCS), PC and smart card integration (PC/SC), Domain Name Service (DNS), and IP Security (IPSec), instead of proprietary technologies such as NTLM, the SAM, WINS, and PPTP (which Win2K will support for backward compatibility). Win2K's use of standards automatically makes it more interoperable with different types of software and hardware solutions. This also enables the user to replace Microsoft components with new cutting edge solutions that employ the same protocols, i.e. third party Virtual Private Network solutions. (Manasi, 1999)

Finally, to answer the challenge of e-commerce, Win2K has support for PKI throughout the OS that includes smart card logon, PKI-based Web access, Virtual Private Networking, EFS, email, and Authenticode. Win2K supports these components through its distributed security services, including Active Directory (AD) services, cryptographic services, Certificate Services, authentication services, secure transport protocols, EFS, and smart cards (Manasi, 1999).

## **D. ACTIVE DIRECTORIES**

Active directory is the directory service included in Window 2000 Server. A directory service provides the means to organize and simplify access to resources of a networked computer system. Directory services are used to uniquely identify users and resources on a network. The resources stored in the directory are known as objects. A directory is a stored collection of information about objects that are related to one another in some way. In an enterprise wide network there are many different objects to be managed. There are printers, users and computers to name a few. Users must be able to locate and use these objects and administrators must be able to manage how these objects can be used. A directory service stores all the information needed to use and manage these objects in a centralized location, simplifying the process of locating and managing these resources.

Windows 2000 AD stores all domain objects, domain security policy and account information within the directory service, and provides this information across all available domain controllers. It groups accounts by Organizational Units (OUs). Organizational Units are containers used to organize objects within a domain into logical administrative groups that mirror the organization's structure (Microsoft Win2K Active Directory Services, 2000). Therefore, rights and privileges can be assigned to a specific property on a specific account within an OU. Now helpdesk personnel can be assigned the specified right to reassign passwords on certain accounts without being granted full administrative privileges. With Win2K, one AD domain can contain more than one million objects and does not require a Primary Domain Controller in most cases (Manasi, 1999).

Windows 2000 domains do not have PDCs. All domain controllers are equal. Changes recorded on any domain controller replicate to the rest. This is an improvement over NT, since all changes to user or computer accounts must have been accomplished on a Primary Domain Controller. This type of replication is referred to as multimaster replication. To accomplish this task, Windows 2000 uses an object called a *site*, which is comparable to an IP subnet under NT. Sites let you separate domains (which are usually based on organizational boundaries) from geographic boundaries (Manasi, 1999).



Active Directories make for much easier administration. To begin with, it is now possible to organize users and computers into a hierarchy that matches the true organizational structure. Within a domain, organizational units (OUs) provide this structure. Domains no longer only have peers and can have parent and child domains too (except for the root domain, which has no parent). Individual administrative privileges can now be assigned at any level. Win2K replaces problematic WINS and broadcast name resolution NetBIOS with dynamic DNS (DDNS). The DNS database can be stored in AD and can be based on the AD domain hierarchy (Manasi, 1999).

New objects and new properties can now be added to existing objects, which means that groups can be nested within other groups, something that was not possible under NT 4.0 (Manasi, 1999). AD even publishes resources such as shared folders in such a way that users don't need to know the physical location of the server where the resources are located. You can also move applications from one server to another without any implications to users. This granularity of control and Win2K's domain support of transitive trust (i.e., if domain A trusts domain B and domain B trusts domain C, then domain A trusts domain C) eliminate the need for basic NT 4.0 flat domain models (e.g., complete trust, master domain). AD's access methods, LDAP and Active Directory Service Interfaces (ADSI), and its hierarchical structure give AD an open architecture and let you integrate it with other directory-enabled OSs and applications such as Novell's Netware. Win2K uses AD as the data store for account and policy information and uses AD's hierarchy to control the flow of policy inheritance. AD relies on the OS to authenticate and control access to AD's objects (Manasi, 1999).

## **E. AUTHENTICATION SERVICES AND KERBEROS**

Unlike the old authentication scheme in NT 4.0 using NT LAN Manager (NTLM), authentication is now based on credentials stored in AD. The default authentication method for users on the network is now based on Kerberos version 5.0. Win2K will still support NTLM for compatibility with NT, and when Win2K systems are used in a workgroup, NTLM authentication will continue to use credentials in the NT Security Accounts Manager (SAM) (Microsoft Win2K Security Technical Reference, 2000). There is no need for users to have both a NTLM account and a Kerberos account.

Another authentication method used by Windows 2000 is Public Key Infrastructure (PKI)-based. This is accomplished by mapping certificates to the proper AD user object. This will be discussed in detail in the section on Certificate Server.

Kerberos Version 5.0 authentication uses the Data Encryption Standard (DES) shared-secret in its protocol. It is called a shared secret because both the client computer and the authentication service on the server it is communicating with both know the one-way encrypted password, which is known as the session key. The Kerberos service issues the ticket (or certificate) that contains the user's name, a session key, and the expiration time for the ticket (Manasi, 1999). The initial ticket lets Win2K authenticate the client on the network so that the client can access resources anywhere on the enterprise network using one logon and password. Kerberos uses several sub-protocols and can operate across different domains. Both the key distribution center (KDC) and the Kerberos authentication service run as a service on each Win2K domain controller. The Kerberos protocol consists of three main components: (1) the central database containing all the information about the users, (2) the principle (or client), and (3) the verifier (or server). (Manasi, 1999)

The major authentication issue, which the Win2K implementation of Kerberos was designed to address, is the replacement of NTLM, which is NT 4.0's vulnerable authentication protocol. It uses password hashes stored in the Security Accounts Manager (SAM) Hive within the Windows NT registry. These hashes are then passed in the clear across the network to the domain controller in order to authenticate users. Alternatively, connecting from an NT system to a Win2K server in an AD domain doesn't invoke the SAM; Win2K will validate the hashed value of the user's password against NTLM hashes stored in the AD user object. An important point to mention is here is Windows 9x systems can be upgraded with the new AD client for Windows 9x, eliminating the need for risky NTLM authentication. This upgrade installs Kerberos V.5 as the default authentication protocol. Kerberos as an authentication protocol is notably more secure than NTLM, and Kerberos is an industry standard. Finally, Kerberos addresses problems that have plagued NTLM—in particular, the slowness and lack of impersonation functionality for multi-tier server applications (Manasi, 1999).

Kerberos is a major change in the way an OS authenticates clients on a Windows network. Kerberos interoperability lets Win2K authenticate even non-Microsoft clients from other platforms (e.g., UNIX), as long as the clients implement Kerberos 5. Kerberos offers enhanced security, efficient authentication, and flexibility.

## **F. CERTIFICATE SERVER**

Certificate Server has been around since NT 4.0 and has provided the basic functionality of a CA for requesting, issuing, publishing, and managing certificates. Certificate Server offered Authenticode authentication and Secure MIME (S/MIME) integration for Exchange Server, but Microsoft geared Certificate Server mostly for public-key-based client authentication to Microsoft Internet Information Server (IIS) (Manasi, 1999). With NT 4.0 administrators had to manually edit text files to control Certificate Server's configuration. Certificate Server also lacked management features important to enterprise usage of PKI, such as tools to customize certificate types and policy settings, and support for only two-level CA hierarchies (inadequate for large-scale PKI deployment)(Manasi, 1999).

In Win2K, Certificate Server's name changes slightly to Certificate Services. Certificate Services is more powerful and better integrated into the rest of the OS (Manasi, 1999). The Microsoft Management Console (MMC) snap-in provides GUI tools for both the client side and server side management tasks. Although Certificate Services can maintain its standalone data store, for full enterprise functionality, Certificate Services uses AD to store and publish certificates (Manasi, 1999). AD maps certificates to users and uses the management features of Group Policy Editor to control for whom, by whom, and for what purposes Certificate Services issues certificates. Certificate Services can also publish certificates in other third-party directories making it even more versatile in the enterprise. Finally, Certificate Services now supports multilevel hierarchies (Manasi, 1999).

## **G. ENCRYPTED FILE SERVICE**

Two areas where critical data can be protected with encryption are on disk and on the network. In NT 4.0, anyone could easily eavesdrop on network data by using sniffers or copy data from disks by using direct access. Win2K's Encrypted File Service (EFS)

lets the user encrypt files at the file-system level by simply selecting a check box. EFS handles encryption and decryption with complete transparency to the user and the application program. EFS integrates with Win2K's PKI and supports data recovery in case the user's private key is lost or unavailable (Manasi, 1999). This, however, can only be accomplished by sending the media to Microsoft or having the encryption key placed in escrow somewhere (Manasi, 1999). EFS will be a nice enhancement for laptop users since these systems are always vulnerable to theft.

## **H. IPSEC**

To protect data across the network, with complete transparency to the user and the application, Win2K uses IPsec. IPsec provides authentication, confidentiality, data integrity, and filtering for TCP/IP traffic (Manasi, 1999). IPsec's implementation is below the application protocol layer and lets any application conduct secure communications without being modified. IPsec is a solid Internet protocol with plenty of industry backing (Manasi, 1999).

Microsoft integrated IPsec well, making it easy to deploy and manage. The AD stores IPsec policy, and IPsec is controlled through the Group Policy Editor. In addition to establishing secure network communication within your enterprise, a Virtual Private Network can be established where users from home or on the road can authenticate to the network and accomplish most tasks. For example, the NPS administrators could require authentication of traffic within individual labs, between labs, encrypted communication between administrators and other departments, and no connections between certain labs and the Internet. Even though these requirements might affect systems in different ways, everything can be centrally managed through AD.

## **I. SUMMARY**

This chapter has focused primarily on the problem this thesis will address, the new features of Window 2000, and the improvements over Windows NT 4.0. The design of the security architecture for Win2K was a monumental undertaking of technology and integration. Microsoft uses proven design concepts such as industry standards, protocols, modularity, and support for PKI to uphold the company's Win2K goals to provide security, scalability, and support. These improvements in Win2K over Windows NT 4.0

are significant and will greatly improve the ability of administrators to implement the security configuration that best fits the organization. The greatest improvements are linked to the Active Directory and the use of Group Policy to configure security settings that are portable across the domain. The next chapter will discuss effective security policy and how it relates to securely configuring operating systems.

THIS PAGE INTENTIONALLY LEFT BLANK

## **II. THE NAVAL POSTGRADUATE SCHOOL'S SECURITY POLICY**

### **A. INTRODUCTION**

The Naval Postgraduate School (NPS) is similar to other organizations in its approach to computing resources and structure. It has end users (students, faculty, and staff) and permanent personnel who manage the available computing resources. The creation of effective security policy is essential to managing these resources and structure. Although the Naval Postgraduate School has an Instruction (NAVPGSCOL INSTRUCTION 5239.1B) on computer security, there is no formal security policy document currently in place. Therefore, this chapter will discuss some approaches to writing effective security policy and make recommendations for a NPS security policy. Once the policy is created, security settings can be defined, which will be covered in Chapter IV.

### **B. DEFINING SECURITY POLICY**

A formal computer security policy is the cornerstone document for the successful implementation of IT resource protection. It assigns program management responsibilities, and provides basic rules, guidelines and definitions for everyone in the organization. According to Noel K Zakin (1995) in his chapter entitled Policies, Standards and Procedures, in the *Computer Security Handbook*, "A policy is a broad statement of management's view and position regarding a particular topic (Zakin, 1995)." He also states that:

This policy statement might then designate the computer security function as management's representative for ensuring that the appropriate protective steps are taken. These steps are in the form of relevant standards, guidelines and procedures (Zakin, 1995).

The above statements lead to a hierarchical development of policy starting with policy then further defining management's intent with standards, guidelines and procedures.

Zakin's (1995) view of security policy is broad in scope and relatively short, containing few specifics. Although it is a view held by several security experts, the author

of this thesis believes that some details need to be highlighted in the security policy to eliminate the requirement to read too many organizational security documents. It is also important that it is well published in the organization and posted where all personnel can easily gain access to it; for example, posted near the top of the organization's intranet web hierarchy would be appropriate. This policy must also be enforceable and understood by all the users to be very useful. If the culture of the organization does not lend itself to enforcing policy in general, then a computer security policy will have very little impact on the members of the organization. The hierarchical approach is typically the way the Department of Defense writes its policy (Roback, 1999).

Another approach to writing effective security policy uses a two-tier structure. The two types of policy are program-level and issue-specific. The primary function of program-level policies is to establish security programs, assign program management's responsibilities, state the organization-wide IT goals and objectives, and provide the basis for enforcement (Roback, 1999). Issue-specific policies also need to be developed in order to identify and define specific areas of concern and to state the organization's position and expectations in relation to them (Roback, 1999). The Naval Postgraduate School's security documentation more closely resembles this approach to security policy development and will be discussed in a later section.

The components of the program-level policy are: purpose, scope, goals, responsibilities, and enforcement. The purpose of this level of policy is to establish the overall program for security. This should include individual responsibilities, firmly establish individual accountability, and establish organizational-wide goals for the security program. It also should be a reminder and place emphasis on management's support for the policy. The scope of the policy should be wide enough to include all of the organization's IT resources to include facilities, hardware, software, information, and personnel. The scope should also include any resources the organization is responsible for even if it is for a short period of time or on loan.

The goals of the organization's security policy should be focused on three main security related needs: integrity, availability, and confidentiality (Roback, 1999). Integrity means that the information is not lost, damaged, or modified by unauthorized



users. Availability means that data and information are accessible to authorized users and can be reached at all times (Kabay, 1996). Confidentiality means that only authorized entities have access to read the information (Microsoft Win2K Security Technical Reference, 2000).

The document within NPS that is closest to this description of an organization's security policy is NAVPGSCOL INSTRUCTION 5239.1B, NPS *Automated Information System (AIS) Security Plan* dated June 26<sup>th</sup> 1998. This document covers scope, purpose, background, individual responsibilities, risk management, training, incident reporting, and software policy. The things it does not cover include guidance on password management, disaster recovery, electronic mail, or a detailed policy statement. The reason these items should be covered is the effects they have on the overall security of the system. For example, if policy does not cover virus protection for e-mail servers, then the entire system can become compromised through an e-mail attachment.

### **C. EFFECTIVE SECURITY POLICY**

The primary security goals of the Naval Postgraduate School can be achieved by taking one initial step; prohibiting everything that is not expressly permitted. What this means in a good security policy is, all actions should initially deny access to all network resources, and then specifically add back access on an explicit functional basis. If the network is implemented in this way, the site security policy will prevent most unwanted actions or procedures.

The first step in developing an effective policy is to identify the Department of the Navy and NPS's expectations of proper computer and network use. In order to accomplish this, all aspects of the school must be considered and agreed upon by the writers of the policy. The security policy that is developed must conform to all existing rules, regulations, and laws that NPS is subject to. For that reason it is necessary to take a look at these and take them into consideration when writing policy. (Sun, 1999)

Another factor influencing the creation of policy are the goals of the organization and how they effect what functionality is required for the users to be able to accomplish their required tasks. Because NPS is an educational institution first, vice a military

installation, the requirements for security are not as stringent. Additionally, different departments and schools within NPS will have different requirements, and these need be considered as well.

Another very important aspect of writing effective security policy is the group designated to write policy. It should be made up of personnel from every functional unit within NPS. In this way, everyone who will be influenced by the policy will have a say in creating it; therefore, buying-in to the policy will be much easier for all parts of the organization.

This group should involve decision makers, technical personnel, and day-to-day users from different levels within the organization (Sun, 1999). The most important of these are the representatives from NPS leadership who have the power to enforce policy. Obviously, personnel from the information technology group are required to advise on the technical implications how the policy will influence the system, and users should be able to voice their concerns on how the policy affects their ability to do their work.

The next step in policy development involves identifying what organizational assets need to be protected. Not everything can have the same level of physical and logical controls, therefore, all protected items need to be prioritized. Some of the items to be considered include: hardware, software, data, documentation, and supplies.

Next, it is important to recognize the threats. According to an *Information Security* magazine survey, the risk from an insider to systems and data is far greater than the risk from external crackers or viruses (Briney, 2000). For example, at least half of all the information security managers surveyed “experienced insider security breaches relating to the unauthorized installation of computing tools, misuse of company resources and abuse of access controls,” and “the number of companies with insiders who stole, sabotaged or intentionally disclosed proprietary data increased by 41% over the last year, while those reporting physical theft of equipment by insiders nearly doubled (Briney, 2000).”

This risk can be managed in three ways. First, policy should dictate proper controls to be implemented to mitigate risk, such as virus scanners and policy on e-mail

attachments. Second, an Intrusion Detection System (IDS) should be implemented to detect internal violations of policy. Third, Users should be trained on proper usage of NPS systems.

The school does not yet have an IDS in place. Therefore, it must rely on policy and the integrity of the users. The user problem is very difficult to quantify because the military tends to trust its users. All students at NPS, except international students, have security clearances, which means they have background investigations, but the staff does not undergo such scrutiny. Still, users should not be given free access to all computer assets and resources. Therefore, controls need to be in place to prevent any unauthorized access to data and resources. Responsibility for auditing must also be included. Procedures for the timely review of audit logs must be addressed as well as a detailed response plan should be documented before any violations occur.

Threats from the outside are also very real and need to be taken seriously. NPS currently has a firewall in place that is effective against most attacks from the outside. The firewall should be covered briefly in the policy, but there should be additional policy development specific to the firewall that covers detailed configuration and administrative information. This document should also contain information about network wide security from a network topology standpoint.

The last consideration in writing effective policy focuses on an often-overlooked area in computer security, physical security. Access to all the important workings of the computer network need to have some level of control. These controls are both physical and electronic. Routers need to be secured behind locked doors and their location should not be made public. Access Control Lists for the school's routers should only be available to select individuals with administrative requirements. All the school's servers need to be secured as well as any databases that may contain sensitive information. If physical security is breached, then all the logical access control measures implemented on the network are useless.

#### **D. CHAPTER SUMMARY**

In this chapter, the basics for writing effective security policy have been addressed. The key take away points are 1) policy needs to be written by a joint team of

users, administrators, and NPS leadership, 2) it needs to address NPS's expectations of proper computer use, 3) it should cover all assets the school wishes to protect, 4) it needs to be visible and read by all users of the system, and 5) be consistent with and comply with DoD and Department of the Navy policy.

Appendix C is a recommended security policy based on the guidelines discussed in this chapter. It covers some information in greater detail than the NAVPGSCOL INSTRUCTION 5239.1B, *NPS Automated Information System (AIS) Security Plan* and some information is not included. It is only a recommendation and should not be treated as official school policy. Next, the discussion will go to the methodology that attackers may use to exploit the NPS network. This discussion will give administrators a better sense of what the template settings are designed to protect against.

### **III. ATTACK METHODOLOGIES AND PREVENTATIVE MEASURES**

#### **A. INTRODUCTION**

Although the focus of this thesis is on a portable user configuration for Windows 2000 Professional (which fulfills a defensive role in network security) it would not be complete without a discussion of what the security settings should defend against, i.e. attackers. For that reason, is important to understand the methodology of the attacker the administrator is attempting to keep out of the system. This chapter will discuss security vulnerabilities from insiders and how Win2K security settings mitigate these vulnerabilities.

#### **B. THE SECURITY RISK FROM INSIDERS AND MITIGATION TECHNIQUES**

##### **1. Attack Methodology**

As discussed in Chapter II, the biggest threat to any organization is not from rouge crackers coming in from the outside, but from employees on the inside who have valid user accounts and access to machines on the network. The motives of these employees range from curiosity to revenge. The security manager's job is to prevent them from gaining access and privileges to machines and data they have no right to access.

First, it is important to understand the methodology used by these individuals so the lab and system administrators can properly secure their systems. Figure 4.1 is an outline of the typical methodology used by insiders to gain access and privileges (Scambray, 2001). For the purposes of this thesis, only scanning, enumeration, gaining access, and escalating privileges will be discussed in any detail.

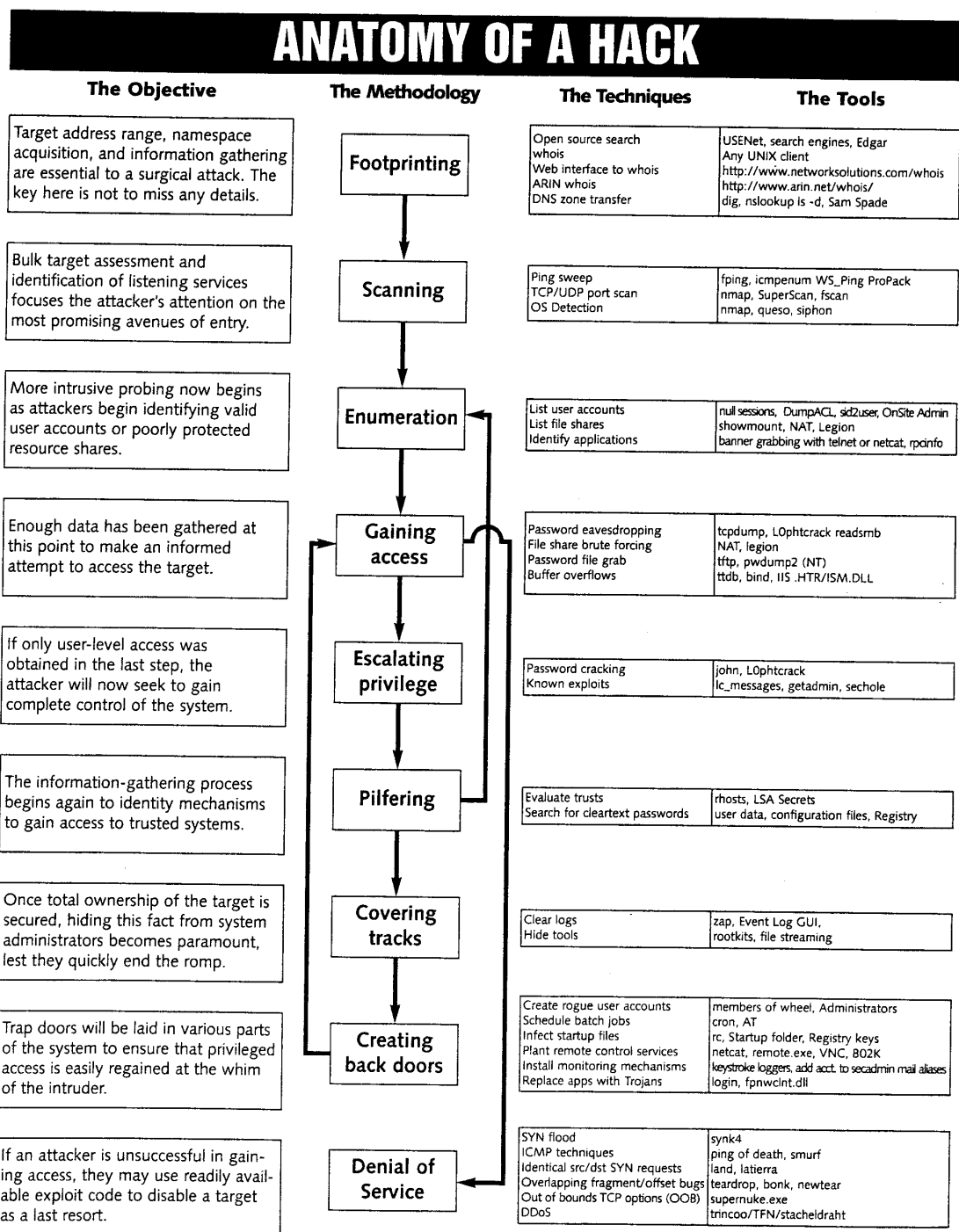


Figure 3.1 The Anatomy of an Attack (from Scambray, 2001)

## 2. Scanning

Port scanning is accomplished by checking each port on a system to determine its status, either listening or closed. A port scan functions by sending a message to each

port, one at a time, and then waiting for a response in order to see if the port is listening. If the port does respond then it can potentially be used to exploit a known vulnerability. All computers connected to the NPS LAN run services that listen to well known or not so well known ports. By scanning these ports, the attacker finds which ports are being listened to by which service. The following is a list of different types of port scans (Scambray, 2001):

- Vanilla: the scanner attempts to connect to all 65,535 ports
- Strobe: a more focused scan looking only for known services to exploit
- Fragmented packets: the scanner sends packet fragments that get through simple packet filters in a firewall
- UDP: the scanner looks for open UDP ports
- Sweep: the scanner connects to the same port on more than one machine
- FTP bounce: the scanner goes through an FTP server in order to disguise the source of the scan
- Stealth scan: the scanner blocks the scanned computer from recording the port scan activities

Currently there is no set standard for services being bound to specific ports, but the computer industry has adapted certain ports for certain services. Generally speaking, port numbers are divided into three ranges: the Well Known Ports (0 - 1023), the Registered Ports (1024 - 49151), and the Dynamic and/or Private Ports (49152 - 65535). For a domain controller running Windows 2000 Server, the following ports are generally used (Microsoft Developer's Network, 2000):

- 21/TCP (Transmission Control Protocol) -- FTP
- 25/TCP -- SMTP (Mail)
- 80/TCP -- HTTP (Web)
- 88/UDP (User Datagram Protocol) -- Kerberos
- 119/TCP -- NNTP (News)
- 135/TCP -- RPC (Remote procedure call (RPC) is a facility that enables a program on one Windows-based computer (the client computer) to invoke the services of another program that is running on a separate Windows-based computer (the server) in a distributed network. RPC is a program-level protocol that can use the communications services of any of the Windows networking protocols, which includes TCP/IP.)
- 137/UDP -- NetBIOS Name Server (The network basic input/output system (NetBIOS) Name Server (NBNS) protocol, which is part of the NetBIOS over TCP/IP (NetBT) family of protocols, provides a means for hostname and address mapping on a NetBIOS-aware network.)

- 139/TCP -- NetBIOS Session Services (NetBIOS Session Services are part of the NetBIOS over TCP/IP (NetBT) family of protocols and is used for server message block (SMB), file sharing, and printing.)
- 389/UDP – LDAP (LDAP is the Lightweight Directory Access Protocol. LDAP is designed to be a standard way of providing access to directory services. In Windows 2000, LDAP is the primary way that the operating system accesses the Active Directory database.)
- 443/TCP – HTTPS (Secure Web)
- 445/TCP – SMB (The SMB protocol is used for file sharing in Microsoft Windows NT and Windows 2000. Windows 2000 enables you to run SMB directly over TCP/IP, without the extra layer of NetBT.)
- 464/TCP -- Kerberos Password V5
- 500/TCP -- ISAKMP
- 563/TCP -- SNEWS
- 593/TCP -- RPC over HTTP
- 636/TCP -- LDAP over SSL
- 1067/TCP -- Installation Bootstrap Service
- 1068/TCP -- Installation Bootstrap Service
- 1645/UDP -- IAS: Internet Authentication Service
- 1646/UDP -- IAS: Internet Authentication Service
- 1701/UDP -- L2TP
- 1723/UDP -- PPTP
- 1812/UDP -- IAS Internet Authentication Service
- 1813/UDP -- IAS Internet Authentication Service
- 3268/TCP -- Microsoft Global Catalog
- 3269/TCP -- Microsoft Global Catalog with LDAP/SSL
- 3389/TCP -- RDP

In order to help secure different systems on the network and limit their vulnerabilities, each service running on each individual system (server or workstation) must be evaluated to determine whether or not it is required to fulfill the intended purpose of the server (i.e. domain controller, print server, file server, etc.). If the service is not required then the service should be disabled, therefore, closing the port the service is listening to. Once a cracker has conducted a successful port scan, the next step is to enumerate information from that system.

### **3. Enumeration**

Enumeration is the ability to gather valid user or group information from a system that will enable a cracker to gain unauthorized access or escalate their privileges. On Windows NT and on Windows 2000 the biggest threat from enumeration comes from



Networked Basic Input Output Service (NetBIOS). It is a requirement for Windows NT networks to function, and is installed by default on Windows 2000 machines to ensure backwards compatibility with other down-level Microsoft clients (a down-level Microsoft client is any older version of the Windows operating system). NetBIOS is not a requirement in a Win2K domain and should be eliminated if possible. Eliminating NetBIOS will be discussed in a later section within this chapter.

In Windows NT it was relatively easy to enumerate information from other Windows NT machines using a NULL session connection. A NULL session connection in Windows NT or Windows 2000 is set up by establishing a non-authenticated connection to port 139 using the following command (`net use \\ IP ADDRESS\IPC$ "" /u:""`). The preceding command connects to the hidden share (IPC\$) at the specified IP address as the built-in anonymous user (`/u:""`) with a null (`""`) password (Scambray, 2001). Port 139 and 445 on Win2K machines will provide information on groups, users, and shares.

It is now important to discuss how Microsoft has approached limiting the user's ability to enumerate information from a Win2K system. Windows 2000 has added a new built-in group, the Authenticated Users group, to limit what the Everyone group could do without limiting the system requirements for authentication. The Authenticated Users group is similar to the Everyone group, except for one important difference: anonymous logon users (or NULL session connections) are never members of the Authenticated Users group; they remain in the Everyone group. Authenticated network connections from any account in the server's domain, or any domain trusted by the server's domain is identified as an Authenticated User. (Microsoft Developer's Network, 2000)

On a new installation of Win2K, anonymous logon users can list domain user names and enumerate share names. This ability is used by several applications and services. For example, listing account names is used by Windows NT Explorer to select from a list of users and groups to grant access to a share (Microsoft Developer's Network, 2000). Within the Win2K security settings there is the ability to restrict anonymous logon users (also known as NULL session connections) from listing account names and enumerating share names. The security setting for this option is found in

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Additional Restrictions for Anonymous Connections. The setting in the registry is named “RestrictAnonymous”.

The purpose of the RestrictAnonymous setting is to establish local policy on whether or not to require authentication in order to perform common enumeration functions. The Server service that provides remote file access to share resources will also use the RestrictAnonymous registry value to control whether anonymous connections can obtain a list of share names (Microsoft Developer’s Network, 2000). Therefore, administrators can set the value of a single registry configuration entry to define how the system responds to enumeration requests by anonymous logons for all requests. When the RestrictAnonymous value is set to 0 (“None. Rely on default permissions”), or the value is not defined, anonymous connections will be able to list account names and enumerate share names. When the RestrictAnonymous value is set to 1 (“Do not allow enumeration of SAM accounts and names”), the “Everyone” group is replaced with the “Authenticated Users” group in each resource’s security permissions. Additionally, anonymous connections from the enumeration tools will receive an access denied error when attempting to get the list of account names.

When the RestrictAnonymous registry value is set to 2 (“No access without explicit anonymous permissions”), the access token built for non-authenticated users does not include the Everyone group, and because of this, the access token no longer has access to those resources which grant permissions to the Everyone group. This means that “Anonymous” must be given explicit permissions to access resources. This can cause undesired behavior because many Windows 2000 services, as well as third-party programs, rely on anonymous access capabilities to perform legitimate tasks. The following tasks are restricted when the RestrictAnonymous registry value is set to 2 on a Windows 2000-based domain controller (Microsoft Developer’s Network, 2000):

- Down-level member workstations or servers are not able to set up a netlogon secure channel.
- Down-level domain controllers in trusting domains are not be able to set up a netlogon secure channel.
- Microsoft Windows NT users are not able to change their passwords after they expire. Also, Macintosh users are not able to change their passwords at all.

- The Browser service is not able to retrieve domain lists or server lists from backup browsers, master browsers or domain master browsers that are running on computers with the RestrictAnonymous registry value set to 2. Because of this, any program that relies on the Browser service does not function properly.

Because of these results, it is not recommended that RestrictAnonymous registry value be set to 2 in mixed-mode environments that include down-level clients. Setting the RestrictAnonymous registry value to 2 should only be considered in Windows 2000 environments only, and after sufficient quality assurance tests have verified that appropriate service levels and program functionality is maintained. (Microsoft Developer's Network, 2000)

Setting RestrictAnonymous does not actually disable NetBIOS nor does it block anonymous connections, it just eliminates the ability to enumerate information over the NetBIOS port 139. In order to eliminate NetBIOS from Windows 2000 open the Network Connections Applet in Control Panel. Then go to Advanced Settings, WINS tab: Disable NetBIOS Over TCP/IP. This will close the NetBIOS ports eliminating the ability of unauthorized users from enumerating information from the network.

In order to close port 445, it is necessary to eliminate File and Print Sharing for Microsoft Networks. In order to do this, go to the Network and Dial-up Connections applet, select Advanced, then Advanced Settings, and deselect File and Print Sharing for Microsoft Networks. This will close the port and close file and printer sharing. (Scambray, 2001)

#### **4. Gaining Access and Escalating Privileges**

Gaining unauthorized access and escalating privileges to systems on the NPS network should be another one of the goals of the system's security configuration. Compromising a Win2K Professional workstation and gaining administrative privileges to that system through a technique discussed next is not too difficult for even a novice cracker if he/she has physical access to the system and can boot from a floppy. Gaining access to a server and escalating privileges on that machine should not be as easy and should be made as difficult as possible. Therefore, one of the primary focuses of server security should be on limiting physical access to them, especially domain controllers. It

is also important to point out that one of the goals of any workstation configuration is to limit its value to any cracker if it is compromised.

There are numerous tools available to escalate privileges on Win2K Professional systems, but one of the easiest is a utility named “chntpw.” This utility takes advantage of the fact that the local administrator account passwords reside in the Security Accounts Manager (SAM) hive of the registry and not in Active Directory as with domain controllers. The utility operates by using the Linux operating system to mount a NTFS partition from a floppy drive. Once the file system is mounted then a new, changed hash of the administrator’s password is injected into the SAM. This works even if SYSKEY is enabled because when the system boots, the new hash of the password is encrypted with SYSKEY (Nordahl-Hegan, 2000). In order to help eliminate this potential problem, password protect the workstation’s BIOS settings to prevent booting from the floppy and lock the case so no one can reset the CMOS pulling the battery and replacing it.

As discussed in the section on enumeration, closing down NetBIOS port 139 and SMB port 445 is crucial in limiting the ability of crackers to enumerate shares and account information. Another critical setting is defining at what level authentication takes place. Kerberos is used by default for authentication, but for backwards compatibility NT LAN Manager (NTLM) in its various forms is also used. If NTLM version 1.0 is used for authentication then password hashes are passed across the network in the clear, thus allowing password sniffing programs like *L0phtcrack* to grab the password hashes (L0phtcrack has the ability to grab SMB packets as they traverse the network). Therefore, it is critical to ensure NTLM version 2 is set as the minimal authentication method.

Setting NTLM v.2.0 as the minimal authentication method is easily done by going to the Security Options section of Computer Configuration \ Windows Settings \ Security Settings \ Local Policies. Set LAN Manager Authentication Level to “Send NTLMv2 response only/refuse LM &NTLM.” This will only allow NTLM version 2 authentication and Kerberos authentication on the network.

If there are any down-level clients on the NPS network a Microsoft add-on can be used to upgrade NTLM to version 2. This support to Windows 9x can be added by

installing the Directory Services Client from the Windows 2000 CD-ROM or by ensuring Windows NT 4.0 is running Service Pack 4 or higher. The name of this tool is the Directory Services Client. It enables several functions, including a feature that lets NT and Win9x clients search Active Directory for information, but the upgrade to NTLM version 2 is the one most critical to the security of the network. To enable a Windows 95/98 client for NTLM 2 authentication, install the Directory Services Client. To activate NTLM 2 on the client, follow these steps (Microsoft Knowledge Base, 2001):

1. Start Registry Editor (Regedit.exe).
2. Locate and click the following key in the registry:  
HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control
3. Create an LSA registry key in the registry key listed above.
4. On the Edit menu, click Add Value, and then add the following registry value:

ValueName: LMCompatibility  
DataType: REG\_DWORD  
Value: 3  
Valid Range: 0,3

Description: This parameter specifies the mode of authentication and session security to be used for network logons. It does not affect interactive logons.

- Level 0 - Send LM and NTLM response; never use NTLM 2 session security. Clients will use LM and NTLM authentication, and never use NTLM 2 session security; domain controllers accept LM, NTLM, and NTLM 2 authentication.
- Level 3 - Send NTLM 2 response only. Clients will use NTLM 2 authentication and use NTLM 2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLM 2 authentication.

The above-mentioned security settings will help close some of the Win2K security vulnerabilities present after a clean installation. These settings should prevent an unauthorized user from enumerating data, escalating privileges and gaining access to systems. Next, this thesis will recommend a set of security settings for the default user profile.

## **C. SUMMARY**

In this chapter the attack methods of port scans, enumeration, gaining access, and privilege escalation were discussed, and how Windows 2000 can help eliminate these vulnerabilities. This discussion was not meant to cover all the methods used by attackers to hack into systems, but introduce some of the more popular techniques. New vulnerabilities are being discovered daily, and the only way to stay abreast of these is to subscribe to security e-mail listings and check security web sites. It is also very important to ensure the latest security patches are installed on the system. The next chapter will show how to implement these recommended settings using the security template provided with the operating system.

## **IV. RECOMMENDATIONS FOR THE SECURITY TEMPLATE AND FINAL THOUGHTS**

### **A. INTRODUCTION**

Although there are a set of general usage guidelines and security procedures for the network administrators to follow, there is still no set enterprise level policy for specific security configuration. This chapter will address how Windows 2000, through the use of a security template, can help address the issue of enterprise wide security and make recommendations for user level security settings. These security settings will be pre-configured in the form of a Windows 2000 security template that is portable to any Windows 2000 Professional machine on the network. Once applied, the template can provide the security manager with a uniform level of security throughout the NPS network. This template is only applicable to Windows 2000 Professional workstations and is not applicable to domain controllers or any server.

### **B. SECURITY SETTINGS USING TEMPLATES**

#### **1. Introduction to Security Templates**

With the introduction of the configurable security template in Windows 2000, system administrators can establish security settings that are portable to numerous machines by implementing Group Policy throughout the network. All the preventative security recommendations discussed in Chapter III will be implemented via settings in the template. Although there are several hundred settings available within each template, this thesis will concentrate on the ones that most effect security. For a more complete discussion of available security templates that come with Win2K see Appendix A, and to see a complete listing of all settings available within the template, refer to Appendix D of this thesis. The security settings are found in the following sections of the template: Computer Configuration \ Windows Settings \ Security Settings \ Account Policies, Local Policies, Event Logs, Restricted Groups, System Services, Registry, and File System. Additionally, there will be a brief discussion about specific settings in User Configuration \ Administrative Templates.

## 2. Security Options

The following settings listed below in Table 4.1 are guidance for the Security Options section of template. They have the most effect on the security of the system the user is logged on to.

Configurable Item	Recommended Setting
Additional Restrictions for Anonymous Connections	No access without explicit anonymous permissions (RestrictAnonymous = 2 See discussion in Chapter IV.)
Allow System to Be Shut Down Without Having to Log On	Disabled (Users must log on system to shut it down, so there is a log of who shut it down.)
Audit Use of Backup and Restore Privilege	Enabled
Clear Virtual Memory Pagefile When System Shuts Down	Enabled
Digitally Sign Client Communication (Always)	Disabled
Digitally Sign Client Communication (When Possible)	Enabled
Digitally Sign Server Communication (Always)	Disabled
Digitally Sign Server Communication (When Possible)	Enabled
Disable CTRL-ALT-DEL Requirement for Logon	Disabled (Users must use WinLogon to begin session)
Do Not Display Last User Name in Logon Screen	Enabled (for multi-user systems)
LAN Manager Authentication Level	Send NTLMv2 responses only/refuse LM & NTLM (See discussion in the section on gaining access and escalating privileges.)
Message Text for Users Attempting to Log On	This is a DoD computer system. This computer system includes all related equipment, networks and network devices (specifically including internet access) are provided for only authorized US Government use. DoD computer systems may be monitored for all lawful purposes; including to ensure that their use is authorized; for management of the system; to facilitate protection against unauthorized access; and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by



	authorized DoD entities to test or verify the security of the system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information including personal information placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes.
Message Title for Users Attempting to Log On	US Government System, Authorized Users Only
Number of Previous Logons to Cache (In Case Domain Controller Is Not Available)	0 (No logon information will be saved on workstations)
Prevent Users From Installing Printer Drivers	Enabled (Will prevent users from adding printers.)
Recovery Console: Allow Automatic Administrative Logon	Disabled
Rename Administrator Account	Rename to something not easily guessed.
Restrict CD-ROM Access to Locally Logged-On User Only	Enabled
Rename Guest Account	Rename to something not easily guessed.
Restrict Floppy Access to Locally Logged-On User Only	Enabled
Secure Channel: Digitally Encrypt or Sign Secure Channel Data (Always)	Disable
Secure Channel: Digitally Encrypt Secure Channel Data (When Possible)	Enabled
Secure Channel: Digitally Sign Secure Channel Data (When Possible)	Enable
Secure Channel: Require Strong (Windows 2000 or Later) Session Key	Disabled (Enable if all systems on the network require 128-bit session key)
Send Unencrypted Password to Connect to Third-Party SMB Servers	Disabled
Shut Down System Immediately If Unable to Log Security Audits	Enabled (Warning: can be used as a DoS attack, but on a workstation not critical)
Strengthen Default Permissions of Global System Objects (e.g. Symbolic Links)	Enabled
Unsigned Driver Installation Behavior	Do not allow

Unsigned Non-Driver Installation Behavior	Do not allow
---	--------------

Table 4.1 Security Options

### 3. Password Policies

The following settings listed in Table 4.2 are recommended for the Password Policy section:

Configurable Items	Recommended Settings
Enforce Password History	24
Maximum Password Age	90
Minimum Password Age	5
Passwords Must Meet Complexity Requirements	Enabled (passwords must contain 3 characters of each of the 4 classes: upper case letters, numbers, lowercase letters, and special characters. Additionally, the user's logon name cannot be used)
Minimum Password Length	10 characters
Store Password Using Reversible Encryption	Disabled

Table 4.2 Password Policy Settings

### 4. Account Lockout Policies

The following settings listed in Table 4.3 are recommended for the Account Lockout Policy section of the template:

Configurable Items	Recommended Settings
Account Lockout Threshold	3 (This should prevent a dictionary type attack where an attacker runs hundreds of passwords at the account at once.)
Account Lockout Duration	20
Reset Account Lockout Threshold After Disabled	(Recommended manual reset of accounts)

Table 4.3 Account Lockout Settings

### 5. Audit Policy

Auditing is a cornerstone security function in any organization. Within Win2K virtually every object and function can be audited, but by default auditing within Win2K is not enabled. Therefore, the following objects listed in Table 5.4 should be audited on all workstations:

Configurable Items	Recommended Settings
Audit Account Logon Events	Success, Failure

Audit Account Management	Success, Failure
Audit Logon Events	Success, Failure
Audit Policy Change	Success, Failure
Audit System Events	Success, Failure
Audit Object Access	Failure
Audit Privilege Use	Failure

Table 4.4 Audit Policy Settings

## 6. Audit Log Settings

In conjunction with the auditing function is ensuring that adequate space is available on the hard drive that contains the audit logs. This is especially important if the system halts on audit failure. As a general rule the primary partition of the system should be at least the log size plus another 50 percent [Cox, 2001].

## 7. User Rights

The User Rights section contains settings that allow functions for users and groups. These rights supplement the built-in abilities that are installed by default. These rights should be reviewed to ensure proper rights and abilities are allowed to groups other than “administrators.” The following settings listed in Table 4.5 are recommended for the User Rights section of the template. These settings are for workstations only and not meant for member servers or domain controllers.

Configurable Items	Recommended Settings
Act as Part of the Operating System	Default
Access This Computer From the Network	Administrators, users
Back Up Files and Directories	Administrators
Bypass traverse checking	Users
Change the System Time	Administrators
Create a Token Object	Default
Create permanent shared object	Default
Create a pagefile	Administrators
Debug Programs	Default
Deny access to this computer from the network	Default
Deny logon as a batch job	Default
Deny logon as a service	Default
Deny logon locally	Default

Enable computer and user accounts to be trusted for delegation	Default
Force Shutdown From a Remote System	Administrators
Generate security audits	Default
Increase quotas	Administrators
Increase Scheduling Priority	Administrators
Load and Unload Device Drivers	Administrators
Lock pages in memory	Default
Logon as a batch job	Default
Log On as a Service	Default
Log On Locally	Administrators, Users
Manage Auditing and Security Log	Administrators
Modify Firmware Environment Values	Administrators
Profile Single Process	Administrators
Profile System Performance	Administrators
Replace a Process Level Token	Default
Remove computer from a docking station	Administrators, Users
Restore Files and Directories	Administrators
Shut Down the System	Administrators, Users
Take ownership of files and other objects	Administrators
Synchronize Directory Service Data	Default

Table 4.5 User Rights Assignment

### C. AREAS FOR FURTHER STUDY AND CONSIDERATION

Just before this thesis was completed, the National Security Agency (NSA) finished their recommended configuration guides for the Windows 2000 operating system. The guide most similar to this thesis is entitled, “Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set.” It comes with additional security templates and has added some additional settings to the Security Options section. One area for further study would be to determine what additional registry settings needed to be added to the template in order to enhance ease of security even further. The NSA guide provides details on how to add additional settings to the template.

Another potential area for further study is Microsoft’s new operating system, Windows XP. Windows XP is currently in its Release Candidate One build and is due for final release in October 2001. It is very similar to Windows 2000, but because it is a new operating system and contains additional features and source code it may also contain additional settings and policies. These new settings and policies should be

explored in detail in order to determine additional recommendations. This thesis did not explore these potential changes.

The next area for further study would be an analysis of IPsec to see how it could be implemented on the NPS network. As discussed in Chapter I, IPsec can be configured to encrypt all traffic on the network, therefore, eliminating potential risk of eavesdropping. The Microsoft implementation of IPsec works on a homogeneous Win2K network, but with all the different systems at NPS, there is a definitive requirement to analyze all systems before IPsec could be deployed.

#### **D. FINAL THOUGHTS**

This chapter has covered recommendations for settings listed in the security template. These recommendations are only that, recommendations. It is the understanding of this author, that SPAWAR will use the NSA guides as guidance for Department of the Navy (DoN) systems, which would lead to the assumption that Electronic Data Systems (EDS) will use them in their configuration for systems attached to the Navy Marine Corps Intranet (NMCI). Therefore, any settings recommended in the NSA document that differ from what is recommended by this document should be assumed to be the recommended DoN settings.

Areas for additional study and analysis were also discussed. Since the Windows 2000 operating system contains so many additional components compared with Windows NT, there are numerous areas not discussed which warrant examination.

The intent of this thesis was to discuss ways to ensure a uniform level of security when the Naval Postgraduate School fully migrates to the Windows 2000 operating system on desktop PCs and servers. It has done that by addressing the Microsoft Windows 2000 security architecture, discussing security policy and how it effects security configurations, providing a security policy for the Naval Postgraduate School, making recommendations on how to translate the Naval Postgraduate School's Security Policy into Windows 2000 security settings, and providing a pre-configured security template for all students attending NPS.



## LIST OF REFERENCES

- Briney, Andy, *Security Breaches*, Information Security, September 2000
- Cole, Eric, Security Essentials Certification 3, SANS Press, 2000
- Cox, Phil and Tom Shelton, *Windows 2000 Security Handbook*, Osborn/McGraw Hill, 2000
- Green, John, Security Essentials Certification 2, SANS Press, 2000
- Kabay, Michel E., The NCSA Guide to Enterprise Security, McGraw-Hill, 1996
- Manasi, Mark, Mastering Windows 2000 Server, Sybex, 1999
- Microsoft, *Active Directory White Paper*, Microsoft Press, 1999
- Microsoft Developer's Network Library*, Microsoft Press, 2000
- Microsoft Knowledge Base, *How to Enable NTLM 2 Authentication for Windows 95/98/2000 and NT*, Microsoft, 2001
- Microsoft, Windows 2000 Security Technical Reference, Microsoft Press, 2000
- Microsoft, Windows 2000 Active Directory Services, Microsoft Press, 2000
- National Computer Security Center, *Department of Defense Trusted Computer System Evaluation Criteria*, , 1985
- National Security Agency's *Guide to Securing Windows NT Networks*, September 6 2000, Version 4.1
- NAVPGSCOL INSTRUCTION 5239.1B, NPS Automated Information System (AIS) Security Plan, Naval Postgraduate School, 1998
- Nordahl-Hagen, Petter, *What Happens When SYSKEY is Installed and How to Get Rid of It*, 2000
- OPNAV INSTRUCTION 5239.1B, Navy Information Assurance Program, US Navy, 1999
- Roback, Ed, Computer and Information Security Policy, *NIST Computer Security Handbook*, US Gov Printing Office, 1999

Scambray, Joel, Stuart McClure, and George Kurtz, *Hacking Exposed*, Network Security Secrets and Solutions, Second Edition, Osborne/McGraw-Hill, 2001

Space and Naval Warfare Systems Command's (SPAWAR) *Secure Windows NT Installation and Configuration Guide*, Windows NT for Navy IT-21, Version 1.3, December 1998

Sun, *How to Develop a Network Security Policy White Paper*, Sun Microsystems

*Windows 2000 Resource Kit*, Microsoft Press, 2000

*Windows 2000 Server*, Microsoft Press, 2000

United States Naval Message, (DTG R 300944Z MAR 97 INFORMATION TECHNOLOGY FOR THE 21<sup>ST</sup> CENTURY)

Zakin, Noel K., Policies, Standards and Procedures, *Computer Security Handbook*, John Wiley and Sons, INC., 1995



## **APPENDIX A: WINDOWS SECURITY TOOL SET**

### **A. INTRODUCTION**

As discussed in Chapter I of this thesis, one of the main advantages of Windows 2000 over Windows NT lies in its ability to link the security configuration tools to the Win2K Active Directory architecture. Microsoft significantly improved the way security is configured on both the workstation and server. This is due to the security configuration tools that are provided with Win2K. This Appendix will provide a brief overview of Security Policy and the Security Configuration Tools Set that is available with Win2K.

### **B. SECURITY POLICY**

Security Policy is treated as an object within Windows 2000. It contains an extensive list of security permissions that apply primarily to the security settings of a domain, computer, or computer desktop (rather than to users). A single Security Policy object can be applied to a single computer or all of the computers in an organizational unit or a domain. Security Policy is applied when an individual computer starts up, and is periodically refreshed if changes are made without restarting.

Stand-alone computers have Security Policy associated with them that can be modified by users (administrators by default) with the appropriate rights, referred to as Local Security Policy. When a computer joins a domain, the domain Security Policy is applied to the local computer. Domain Security Policy will override any changes made to the Local Security Policy. Security Policy lets you apply a single security profile to multiple computers. It enforces consistency and provides easy administration. Security Policy objects contain permissions and parameters that implement multiple types of security strategies. Security Policy is installed by default on local computers. However, Active Directory must be installed on a server before you can edit and apply domain-wide Security Policy objects.

Security Policy in Active Directory is configurable by administrators with the proper access. This is accomplished by defining security settings in a Group Policy Object (GPO) that are associated with a domain or an organizational unit (OU). Security

settings that are defined for a domain or OU apply to all machines that are contained in that domain or OU.

Security policy is also established on the local machine by default. However, this local machine policy only contains security settings for two security areas, Account Policies and Local Policies (other security areas will be discussed in detail in a later section). While local security policy may only be established for Account Policies and Local Policies, other security areas may be configured on a local machine through the use of various other tools.

Security settings that are defined in Active Directory always override any security settings on the local machine. Security settings for an OU always override security settings defined in any parent OUs or on the domain itself. The following is the order of precedence that determines how security settings are applied to a specific machine from lowest to highest: 1) Local security policy, 2) Domain policy, 3) OU policy, and 4) OU policy (for the OU that the machine is contained in) (Microsoft Developer's Network, 2000).

## **C. WINDOWS 2000 WORKSTATIONS AND SERVERS**

The way the Security Policy is applied on Workstations, servers and domain controllers, and which security areas are implemented at what level is discussed next.

### **1. Windows 2000 Professional and Member Servers**

When Win2K workstations and servers (but not domain controllers) are installed, Local Security Policy is implemented by default. This policy defines security settings for all Account Policies and Local Policies with the following exceptions:

***Kerberos Policy*** - A Kerberos policy is not defined because Kerberos settings are domain-wide and cannot be configured on individual machines (Microsoft Developer's Network, 2000).

***Disable CTRL+ALT+DEL requirement for logon*** - The CTRL+ALT+DEL requirement is not defined because this setting differs depending on whether or not the machine is joined to a domain (Microsoft Developer's Network, 2000).

***Rename Administrator Account and Rename Guest Account*** - The Administrator and Guest account names are not defined because these

accounts are not "renamed" by default (Microsoft Developer's Network, 2000).

***Driver and Non-Driver Signing Policy*** - A signing policy is not established because there are specific mechanisms for configuring these values during unattended setup (Microsoft Developer's Network, 2000).

***Nonexistent registry keys on upgrades*** - for upgraded machines, there may be several registry values that did not exist on the previous Windows NT4 configuration. No attempt is made to create these registry values during the upgrade process, so any policy associated with these registry values remains undefined (Microsoft Developer's Network, 2000).

In any situation where the policy is not defined for a particular value, the system always assumes some default value. This means that the policy for that specific setting has not been set by a user with the proper access. An example of this would be where a machine is joined to a domain, and last user name is left in the login box. This setting is the default upon installation, but it is not defined by policy. To change this default behavior, or to establish a policy regarding this behavior (even if it's the same as the default behavior), the setting for this security option should be defined.

It is important to note that maintaining a defined state for all local policies ensures that a system is not altered with an Active Directory based setting that has since been undefined (Microsoft Developer's Network, 2000). The following is an example taken from the Microsoft Developer Network July 2000:

Consider the security option *Additional restrictions for anonymous connections*. By default, there are no additional restrictions for anonymous connections, and this is reflected in the default local security policy. Now assume that an administrator decides to define additional restrictions for all machines in the domain. The administrator modifies the Default Domain GPO and configures this security option. Subsequently it is determined that certain applications no longer function properly with these restrictions so the administrator "undefines" the domain-level policy. If there were no local policy definition for this security option, then the domain-level policy would remain in effect even after it was "undefined". By having a local policy defined, that local

policy setting becomes effective when the domain-level policy is not defined.

## **2. Windows 2000 Domain Controllers**

In Windows 2000, Domain Controllers Account Policies (Password, Lockout, and Kerberos Settings) are all defined in the Default Domain GPO (Microsoft Developer's Network, 2000). Domain controllers are also subject to the Default Domain GPO. Therefore, all Windows 2000 machines in the domain obtain the same password and lockout policies for their local Security Accounts Manager (SAM) database even though they have their own default local account policies defined (Microsoft Developer's Network, 2000). As mentioned above, this is because domain-level policies have precedence over local policies. It is important to remember that a policy defined for a specific OU has priority over a domain policy, therefore, allowing an override of the domain policy by including a specific server or workstation in an OU with different policy settings.

Since Audit Policy and User Rights are also defined by default in the Default Domain Controller GPO, all domain controllers have the same Audit and User Rights policy. The Security Options subcategory of local policies is not defined in the Default Domain Controller GPO because it is possible, and may be desirable, to have different values defined for individual domain controllers (Microsoft Developer's Network, 2000). It is recommended that the policy settings for Event Log Settings, Restricted Groups, System Services, Registry access control lists (ACLs), and File System ACLs be defined on Domains or OUs in Active Directory (Microsoft Developer's Network, 2000). This will allow administrators with the proper permissions to protect the Win2K system directories in a certain way or that members of the local Administrators group on all machines only contain a certain set of individuals. This is because these security settings are not considered part of local security policy, and no local security policy is maintained for these security areas.

## D. WINDOWS SECURITY CONFIGURATION AND ANALYSIS TOOL

With Windows NT 4.0 the tools available to manage and configure the security of the operating system were always readily available, but not in an organized manner. Through various registry hacks, file permission settings and tools such as User Manager for Domains, a system administrator could feel relatively secure about their domain. What Windows 2000 has done is consolidate and organize all the tools required to secure a system or domain. These tools are available within the Microsoft Management Console (MMC). These tools also simplify the construction and deployment of various security configurations across multiple systems. The tools are scalable and the security policies that can be created can be applied to individual systems or deploy them across multiple domains or Organizational Units (OUs) via Group Policy Objects (GPOs) (Microsoft Win2K Security Technical Reference, 2000). The policies can also be exported or imported allowing their deployment across a single domain or the entire enterprise. These tools include the Security Configuration and Analysis Snap-in, the `secedit.exe` command line tool, the Security Settings extension to the Group Policy editor, and the Security Templates snap-in.

The Windows Security Configuration and Analysis Snap-in is a tool that allows the administrator to configure specific security settings, test them against the security settings on the local machine, and then apply those settings if required. Although these settings only affect the local machine and cannot be applied to the domain or any organizational unit, it is important to understand how this tool works because it is the primary tool used to test configurations that can be applied to all the machines in the domain or OU.

The Configuration and Analysis Snap-in tool is accessible via the Microsoft Management Console (MMC). In order to open a MMC, go to the run command and type in “mmc” then click OK. From the MMC menu, click *add/remove snap-in* and then click the *add* button. Select and add *Configuration and Analysis* and *Security Templates*. The MMC can be saved to any name the administrator/user wishes.

Once the MMC is created, a database must be opened. The database used by the snap-in contains all the existing security properties available for a Windows 2000 Local machine. This is the database that will be compared to security settings on the local machine, but not the domain. The user has the option of opening an existing database or creating a new one. Right click on *Security Configuration and Analysis* and select *Open Database*. Then choose between opening an existing database and creating a new one by entering the name of the database in the filename box. If choosing to create a new one and after clicking *Open*, the Import Template dialog box appears. This is where the security configuration entries come from to populate the database. These templates can either be imported in their entirety or merged with other templates. The template chosen should contain the configuration settings that most closely resemble the level of security the user is trying to obtain.

#### **E. DEFAULT SECURITY TEMPLATES**

The Security Templates snap-in enables the administrator to define, edit, and save secure templates. The templates are text based files which can be read by any text editor, but it is not recommended that they be modified with a text editor since that can easily render them unusable by the Security configuration Service Engine (Microsoft Win2K Security Technical Reference, 2000).

Windows comes with a complete set of security templates. These templates ease the administrative burden of developing a security policy for a new install. There are two categories of templates, one is the Basic Template and the second is the Secure Template. The Basic or Default template is applied to the system when a clean install is performed.

The Basic security templates apply the Windows 2000 default security settings for all security areas with the exception of user rights and groups (Microsoft Win2K Security Technical Reference, 2000). The Basic template is applied to a Windows NT computer that has been upgraded to Windows 2000. This will bring the upgraded computer in line with the new Windows 2000 default security settings that are applied only to clean-installed computers. Figure 1 is a Windows 2000 screen shot of all the templates found in Windows 2000 by default, and the following is a list of the basic security templates:

- Basicwk.inf (for computers running Windows 2000 professional)

- Basicsv.inf (for computers running Windows 2000 server)
- Basicdc.inf (for domain controllers running Windows 2000 Server)
- OCFiles.inf (for standalone or member servers, not domain controllers)
- OCFilesw.inf (for computers running Windows 2000 professional)

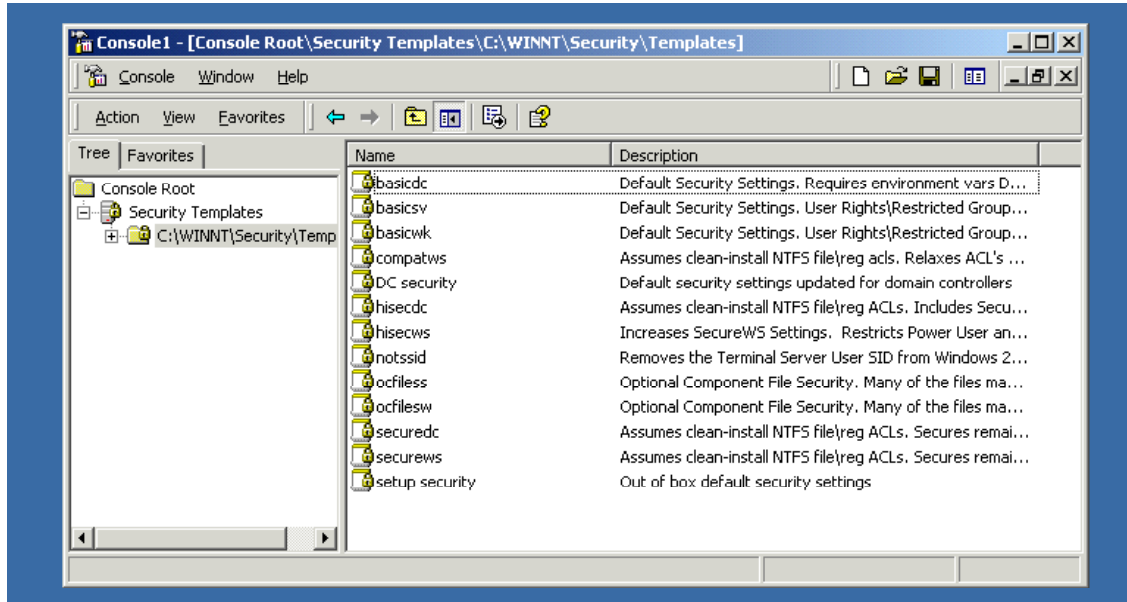


Figure 1 Screen Shot of Windows 2000 Security Templates

With these basic templates, user and group rights are not affected because these settings are often modified by applications (Microsoft Win2K Security Technical Reference, 2000). The OCFiles templates contain default security settings for all optional component files that might or might not be installed during or after the initial setup is run. Since not all the files specified in the OCFiles template can exist on a given system, the log files will probably contain numerous warning messages reflecting that the file did not exist and thus security could not be set on it (Microsoft Win2K Security Technical Reference, 2000).

The Secure Template comes in three varieties, compatible, secure, and highly secure. These templates are intended to modify the default security settings. These are intended for machines that are already running the default templates and do not include the default settings plus the modified security settings.

### 1. Conpat.inf

This template is for workstations or servers, but not domain controllers. The default Windows 2000 access permissions are assigned to three primary groups: Users,

Power Users, and Administrators. The default permissions for the Users group have been considerably tightened over previous versions of Windows NT, providing for a more secure operating system environment. However, this has resulted in non-certified applications, including most legacy applications, failing to run properly. Therefore in order to run these legacy applications the user must have the same access as the access granted in the Power Users group. (Microsoft Developer's Network, 2000)

By default, users on Win2K workstations are Power Users. Administrators might not want their users to have the access granted to Power Users. This is because users have additional capabilities, such as the ability to create shares. These abilities also grant access control settings necessary to run legacy applications. The Compatible template "opens up" the default access control policy for the Users group in a manner that is consistent with the requirements of most legacy applications (Microsoft Developer's Network, 2000). For example, Microsoft Office 97 SR1 runs successfully as a Power User, or as a User under the Compatible configuration. However, Office 97 does not run successfully as a clean-installed User using the default settings defined in the basicwk.inf template. Note that Microsoft Office 2000 runs successfully as a clean-installed User because it is compliant with the Windows 2000 application specification (Microsoft Win2K Security Technical Reference, 2000). This template is supplied so administrators can allow their users access to legacy software, but not allow the User Group the elevated privileges allowed the Power Users Group in Windows 2000. The Power Users Group in Windows 2000 has even more privileges than they did under Windows NT 4.0. A computer that is configured with the Compatible template must not be considered a secure installation.

## **2. Securews.inf and Securedc.inf**

The Securews.inf is for Windows 2000 Professional and Windows 2000 Server and Securedc.inf template is for Windows 2000 domain controllers. The Secure template modifies settings that are less likely to have an impact on application functionality and more of an impact on the operational behavior of the operating system and its network protocols. Additionally, they provide security for areas of the operating system not covered by default access permissions, including increased security settings for account



policy, auditing, and well-known security relevant registry keys (Microsoft Win2K Security Technical Reference, 2000).

The Secure template provides recommendations that are distinct from the access control policy that has been defined in the default configuration. The Secure template does not modify any ACLs, but it does remove all members of the Power Users group. Additionally, permissions to files system objects are not affected with these templates.

### **3. Hisecdc.inf and Hisecws.inf**

The Highly Secure templates include hisecdc.inf and hisecws.inf. This template is used when there is a requirement for increased security beyond what is defined in the Secure Template. The High Secure template configures many operational parameters to their extreme values without regard for performance, operational ease of use, or connectivity with clients using third-party or earlier versions of NTLM (Microsoft Developer's Network, 2000). These two templates remove all members of the Power Users Group, and also include all the settings listed in the Secure templates plus security settings for IPSec and added security for network communications.

## **F. ANALYZING AND CONFIGURING THE LOCAL MACHINE**

The Configuration and Analysis Tool takes the designated database, which has been populated with a template [Remember that on a clean installation the default template is applied to the local machine.], and compares it to what is currently applied to the local machine. In order to accomplish this, right click on the *Security Configuration and Analysis* node and select *Analyze Computer Now* and the computer will run and analysis and show its progress. Figure 2 is a screen shot of the export option within the Security Configuration and Analysis Tool.

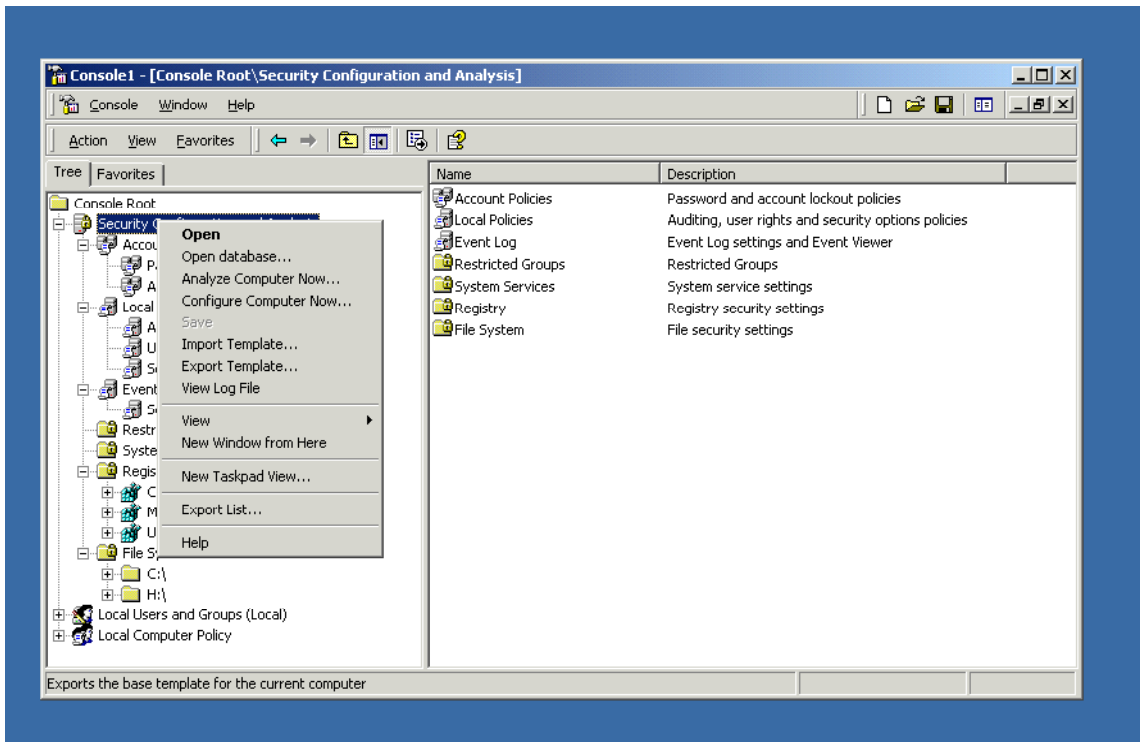


Figure 2 Screen Shot of Export option within Security Configuration and Analysis Tool

The analysis tool will compare the two configuration settings and display the outcome in the right pane of the MMC. It will list the different policy settings, and then in the next two columns list the database settings and the local computer settings. Individual security settings will be flagged with an icon that will change, depending on whether or not the actual security settings are the same or different from those include in the database. The administrator will also be informed if the settings have been configured at all. A green check mark indicates that the current settings are the same as those set in the database. A red “x” indicates that there is a conflict and a generic icon indicates that the setting has not yet been defined in the database.

The administrator can now apply any needed changes to the database and then apply settings in the database to the local machine by 1) simply right clicking on *Security Configuration and Analysis* under the console root in the MMC, and then 2) just clicking on *Configure Computer Now...* and the settings in the template are automatically applied. The settings can also be exported to a template by just right clicking on *Security Configuration and Analysis* under the console root in the MMC and choosing *Export*

*Template.* The exported template is saved as an .inf file and can be imported to any other computer.

## G. SECURITY CONFIGURATION AND ANALYSIS AREAS

The most powerful aspect of the tool is the bringing together in one workspace many components that were spread throughout many different programs under Windows NT 4.0. The following are the categories that allow granular manipulation of the security configuration: Account Policies, Local policies, Event Log, Restricted Groups, System Services, Registry, and File System. Figure 3 is a screen shot of the security configuration areas available in Windows 2000.

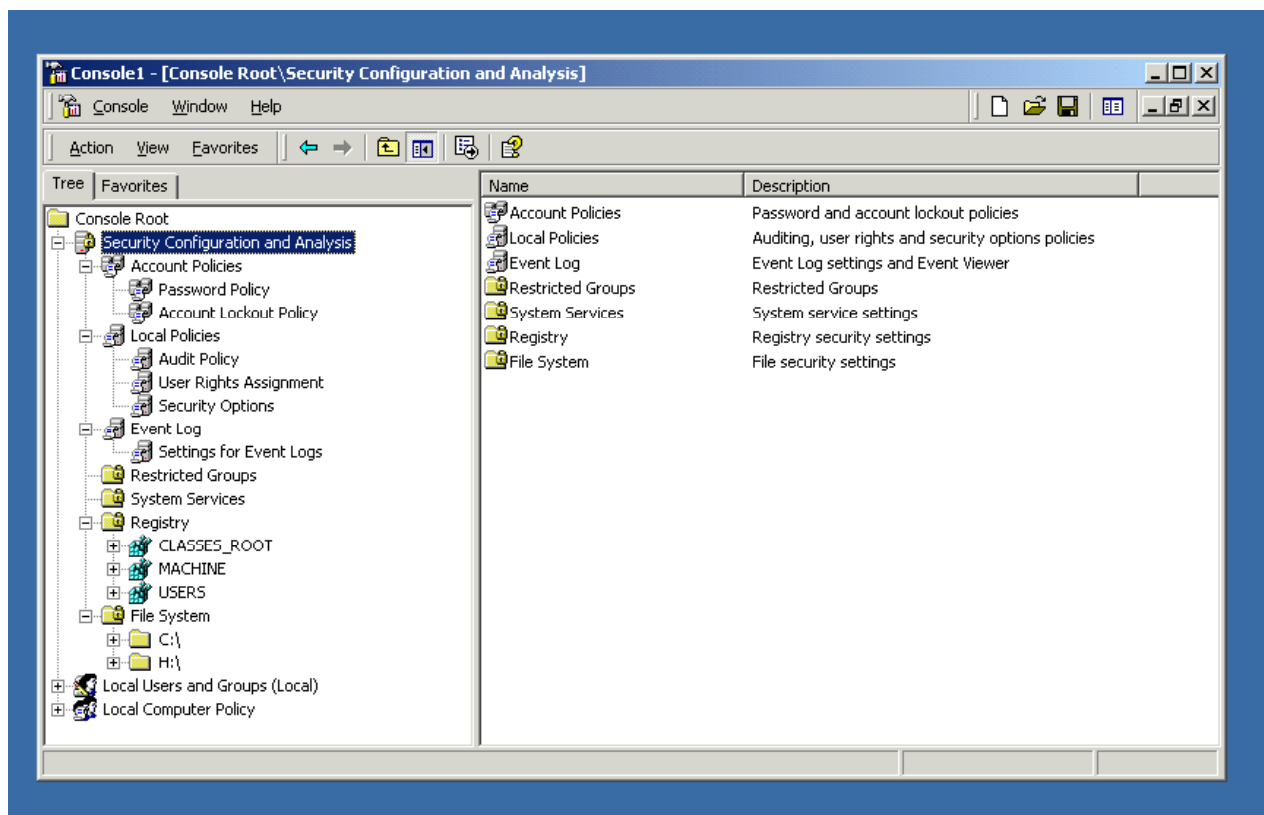


Figure 3 Screen Shot of Security Configuration and Analysis Areas

### 1. Account Policies

The Account Policies node includes those configuration variables that you formerly manipulated in the User Manager for Domains applet in NT 4.0. These policies cover areas of security regarding users and accounts. The three sub nodes include the Password Policy node, Kerberos node and Account Lockout node. In the **Password policy node**, the administrator can set the minimum and maximum password age,

uniqueness and length. This policy can be modified to meet the specific requirements of the organization. Also requirements can be set for users to use complex passwords and prevent the reuse of passwords. Default settings for Password Policies on a local computer are described in Table 1.

<b>Policy</b>	<b>Local Setting</b>
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Passwords must meet complexity requirements	Disabled
Store password using reversible encryption for all users in the domain	Disabled

Table 1 Password Policy Table (from Microsoft Developer's Network, 2000)

The **Account Lockout Policy** allows you to set the lockout durations and reset by time or administrator. There are also settings for user accounts to be locked out after a specific number of failed logon attempts. Default settings for Account Lockout Policies on a local computer are described in Table 2.

<b>Policy</b>	<b>Local Setting</b>
Account lockout duration	Not defined
Account lockout threshold	0 invalid logon attempts
Reset account lockout counter after	Not defined

Table 2 Account Lockout Policy Table (from Microsoft Developer's Network, 2000)

## 2. Kerberos Policy

The **Kerberos Policy** configures the security settings for Kerberos authentication, such as the Kerberos ticket lifetime. Kerberos settings are domain wide and are not applied to any specific machine. These settings are defined in the domain controller GPO. Default settings for Kerberos Policies on a local computer are described in Table 3.

<b>Policy</b>	<b>Local Setting</b>
Enforce user logon restrictions	Not defined
Maximum lifetime for service ticket	Not defined
Maximum lifetime for user ticket	Not defined
Maximum lifetime for user ticket renewal	Not defined
Maximum tolerance for computer clock	Not defined

Table 3 Kerberos Policy Table

### 3. Local Policies

The sub nodes of Local Policies include the Audit Policy, User Rights Assignment, and the Security Options node. The **Security Options node** offers the administrator the ability to manipulate settings that used to be only changeable via the registry in Windows 4.0. These include a variety of configuration settings, such as whether or not to display last logged on user and the right to eject removable NTFS formatted media. These individual settings are discussed at length in a following section. Default settings for Security Options Policies on a local computer are described in Table 4.

<b>Policy</b>	<b>Local Setting</b>
Additional restrictions for anonymous connections	Rely on default permissions (none set by default)
Allow server operators to schedule tasks (domain controllers only)	Not defined
Allow system to be shut down without having to log on	Enabled
Allowed to eject removable NTFS media	Administrators
Amount of idle time required before disconnecting session	15 minutes
Audit the access of global system objects	Disabled
Audit use of Backup and	Disabled

Restore privilege	
Automatically log off users when logon time expires (local)	Enabled
Clear virtual memory pagefile when system shuts down	Disabled
Digitally sign client communication (always)	Disabled
Digitally sign client communication (when possible)	Enabled
Digitally sign server communication (always)	Disabled
Digitally sign server communication (when possible)	Disabled
Disable CTRL+ALT+DEL requirement for logon	Not defined
Do not display last user name in logon screen	Disabled
LAN Manager Authentication Level	Send LM and NTLM responses
Message text for users attempting to log on	<None>
Message title for users attempting to log on	<None>
Number of previous logons to cache (in case domain controller is not available)	10 logons
Prevent system maintenance of computer account password	Disabled
Prevent users from installing printer drivers	Disabled
Prompt user to change password before expiration	14 days
Recovery Console: Allow automatic administrative logon	Disabled
Recovery Console: Allow floppy copy and access to all drives and all folders	Disabled
Rename administrator account	Not defined
Rename guest account	Not defined
Restrict CD-ROM access to locally logged-on user only	Disabled
Restrict floppy access to locally logged-on user only	Disabled

Secure channel: Digitally encrypt or sign secure channel data (always)	Disabled
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled
Secure channel: Digitally sign secure channel data (when possible)	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Disabled
Send unencrypted password to connect to third-party SMB servers	Disabled
Shut down system immediately if unable to log security audits	Disabled
Smart card removal behavior	No Action
Strengthen default permissions of global system objects (for example, Symbolic Links)	Enabled
Unsigned driver installation behavior	Not defined
Unsigned non-driver installation behavior	Not defined

Table 4 Security Options Policy Table (from Microsoft Developer's Network, 2000)

#### 4. Audit Policy

**Audit policy** lets the administrator establish the overall audit policy settings for the particular system or GPO. Default settings for Audit Policies on a local computer are described in Table 5.

<b>Policy</b>	<b>Local Setting</b>
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing

Audit system events	No auditing
---------------------	-------------

Table 5 Audit Policy Table (from Microsoft Developer's Network, 2000)

## 5. User Rights

**User Rights Assignment** enables the administrator to specify the rights for user account and security groups including the rights of users or groups to perform specific security related management tasks. Default settings for User Rights Assignment Policies on a local computer are described in Table 6.

Policy	Local Setting
Access this computer from the network	Everyone
Act as part of the operating system	<None>
Add workstations to domain	<None>
Back up files and directories	Backup Operators
Bypass traverse checking	Everyone
Change the system time	Power Users
Create a pagefile	Administrators
Create a token object	<None>
Create permanent shared objects	<None>
Debug programs	Administrators
Deny access to this computer from the network	<None>
Deny logon as a batch job	<None>
Deny logon as a service	<None>
Deny logon locally	<None>
Enable computer and user accounts to be trusted for delegation	<None>
Force shutdown from a remote system	Administrators
Generate security audits	<None>
Increase quotas	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	<None>
Log on as a batch job	<None>



Log on as a service	<None>
Log on locally	Computer Domain\Guest
log Manage auditing and security	Administrators
values Modify firmware environment	Administrators
Profile single process	Power Users
Profile system performance	Administrators
Remove computer from docking station	Users
Replace a process level token	<None>
Restore files and directories	Backup Operators
Shut down the system	Users
Synchronize directory service data	<None>
Take ownership of files or other objects	Administrators

Table 6 User Rights Assignment Policy Table (from Microsoft Developer's Network, 2000)

## 6. Event Log

The Event Log node allow the administrator to set maximum log sizes, configure guest access to the event log, and whether or not the computer should be shut down when the security log is full. Default settings for Event Log Policies on a local computer are described in Table 7.

Policy	Local Setting
Maximum application log size	Not defined
Maximum security log size	5120 Kilobytes
Maximum system log size	Not defined
Restrict guest access to application log	Enabled
Restrict guest access to security log	Enabled
Restrict guest access to system log	Enabled
Retain application log	Not defined
Retain security log	Not defined
Retain system log	Not defined
Retention method for application log	Not defined
Retention method for security log	As needed
Retention method for system log	Not defined

Shut down computer when security log is full	Not defined
--	-------------

Table 7 Event Log Policy Table

## 7. Restricted Groups

Through these settings the administrator can centrally control members of groups. A group membership list of approved members can be configured then applied to the local machine. Therefore, when a restricted group is applied to a machine, only the restricted groups that are local to the machine will be configured.

## 8. System Services

The System Services node allows the administrator to define all the security parameters of all the system services to include whether a service startup should be automatic, manual or disabled; and which user account has access to each service. This defines whether a user can start, stop, pause, or delete a service, or is restricted to read or write access only. The administrator can also set audit levels for the services to aid in detecting intruders.

## 9. Registry

The Registry node allows the administrator to set access restrictions on individual registry keys. It can also specify the types of accesses for which auditing is desired.

## 10. File Systems

The File System node allows the administrator to set folder and file permissions on file system objects; it can also specify the types of accesses for which auditing is desired. Additionally, this allows the administrator to apply a security template to a machine and restore all file and folder permissions to their original settings.

## 11. Encrypted File System

Default settings for the Encrypted Data Recovery Agent Policy are described in Table 8.

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status
Administrator	Administrator	10/8/99	File Recovery	<None>	<None>

Table 8 Encrypted Data Recovery Agent Policy (from Microsoft Developer's Network, 2000)

## 12. Internet Protocol Security Policies on Local Computer

Default settings for Internet Protocol Security Policies on a local computer are described in Table 9.

Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (unsecured). Use the default response rule to negotiate with servers that request security. Only the requested protocol and port traffic with that server is secured.	No
Secure Server (Require Security)	For all IP traffic, always require security using Kerberos trust. Do not allow unsecured communication with untrusted clients.	No
Server (Request Security)	For all IP traffic, always request security using Kerberos trust. Allow unsecured communication with clients that do not respond to request.	No

Table 9 Internet Protocol Security Policies on Local Computer (from Microsoft Developer's Network, 2000)

## H. SUMMARY OF SECURITY TOOL SET

This Appendix has addressed all the settings that can be manipulated by the Security Configuration Tool set. These areas, especially the Security Options area, are the key to ensuring the proper security settings are in place on machines for different purposes. Once the administrator feels comfortable with all the settings and what they mean, (see Appendix D) then the exact configuration can be put in place on workstations, Servers, and Domain Controllers. The security configuration tools available with Win2K should greatly enhance the administrator's ability to secure his/her enterprise.

THIS PAGE INTENTIONALLY LEFT BLANK

## **APPENDIX B. SECURITY SETTINGS BY POLICY**

The following section lists the policies that are enabled, disabled, or not set. This allows the administrator to view the settings which are set and which settings are not set with the default configuration. This appendix also contains the capabilities granted to power users and compares them to the capabilities granted to administrators. The following information is from the Microsoft Developers Network, July 2000 edition.

### **A. ENABLED**

The following policies are enabled by default when you install Windows 2000 Professional on a stand-alone computer:

- Allow system to be shut down without having to log on.
- Automatically log off users when logon time expires (local).
- Digitally sign client communication (when possible).
- Secure channel: Digitally encrypt secure channel data (when possible).
- Secure channel: Digitally sign secure channel data (when possible).
- Strengthen default permissions of global system objects (for example, Symbolic Links).

### **B. DISABLED**

The following policies are disabled by default when you install Windows 2000 Professional on a stand-alone computer:

- Passwords must meet complexity requirements.
- Store password using reversible encryption for all users in the domain.
- Account lockout threshold.
- Audit the access of global system objects.
- Audit use of Backup and Restore privilege.
- Clear virtual memory pagefile when system shuts down.
- Digitally sign client communication (always).
- Digitally sign server communication (always).
- Digitally sign server communication (when possible).
- Do not display last user name on logon screen.
- Prevent system maintenance of computer account password.
- Prevent users from installing printer drivers.
- Recovery Console: Allow automatic administrative logon.
- Recovery Console: Allow floppy copy and access to all drives and all folders.
- Restrict CD-ROM access to locally logged-on user only.

- Restrict floppy access to locally logged-on user only.
- Secure channel: Digitally encrypt or sign secure channel data (always).
- Secure channel: Require strong (Windows 2000 or later) session key.
- Send unencrypted password to connect to third-party SMB servers.
- Shut down system immediately if unable to log security audits.
- Additional restrictions for anonymous connections.
- Message text for users attempting to log on.
- Message title for users attempting to log on.
- Smart card removal behavior.
- Audit account logon events.
- Audit account management.
- Audit logon events.
- Audit object access.
- Audit policy change.
- Audit privilege use.
- Audit process tracking.
- Audit system events.

### **C. NOT DEFINED**

By default, the following policies are not defined. This does not mean that values are not set for these parameters on the system. It just means that there is no local policy defined for these parameters.

- Account lockout duration.
- Reset account lockout counter after.
- Audit directory service access.
- Allow server operators to schedule tasks (domain controllers only).
- Disable CTRL+ALT+DEL requirement for logon.
- Rename administrator account.
- Rename guest account.
- Unsigned driver installation behavior.
- Unsigned non-driver installation behavior.

### **D. NOT GRANTED**

By default, the following policies are not granted to any particular group when you clean-install Windows 2000 Professional on a stand-alone computer:

- Act as part of the operating system.
- Add workstations to domain.
- Create a token object.
- Create permanent shared objects.

- Deny access to this computer from the network.
- Deny logon as a batch job.
- Deny logon as a service.
- Deny logon locally.
- Enable computer and user accounts to be trusted for delegation.
- Generate security audits.
- Lock pages in memory.
- Log on as a batch job.
- Log on as a service.
- Replace a process level token.
- Synchronize directory service data.

## **E. COMPARISON OF GROUP CAPABILITIES**

By default, a member of the Administrators group can:

- Install the operating system.
- Install or configure hardware device drivers, although Power Users are allowed to install printer drivers.
- Install system services.
- Install Service Packs and Windows Updates.
- Upgrade the operating system.
- Repair the operating system.
- Install applications that modify Windows system files.
- Configure password policy.
- Configure audit policy.
- Manage security logs.
- Create administrative shares.
- Create administrative accounts.
- Modify groups or accounts created by other users.
- Remotely access the registry.
- Stop or start any service.
- Configure services.
- Increase quotas.
- Increase execution priorities
- Remotely shut down the system.
- Take ownership of arbitrary objects.
- Assign rights to members of the Users group.
- Override a locked computer.
- Format a hard disk drive.
- Modify system-wide environment variables
- Access the private data of members of the Users group.
- Back up and restore files.

By default, a member of the Power Users group can:

- Create local users and groups.
- Modify users and groups that they have created.
- Create and delete non-administrator file shares.
- Create, manage, delete, and share local printers.
- Change system time (default user right).
- Stop or start non-auto-started services.

By default, members of the Power Users group are granted the following permissions:

- Modify access to the Program Files directory.
- Modify access to many locations within the HKEY\_LOCAL\_MACHINE \Software registry hive.
- Write access to most system directories including %windir% and %windir%\system32.
- These permissions allow members of the Power Users group to:
- Perform per-computer installation of many applications. For example, applications that do not modify Windows system files or do not modify HKEY\_LOCAL\_MACHINE \System.
- Run legacy applications that improperly store per-user data in per-computer locations (without receiving error messages).
- Unfortunately, these permissions also allow members of the Power Users group to:
- Plant Trojan horses that, if executed by administrators or other users, can compromise system and data security.
- Make system-wide operating system and application changes that affect other users of the system.



## **APPENDIX C: RECOMMENDED NPS SECURITY POLICY**

The following Appendix is a recommended security policy based on the perceived needs of the Naval Postgraduate School. It follows the recommendations brought forward in Chapter III of this thesis.

### **A. FORWARD**

The Naval Postgraduate School's primary mission is graduate education. The ability to support this mission has grown enormously through the use of information systems and computers. The Naval Postgraduate School has a significant investment in information resources, both in the areas of hardware and software. While the value of equipment such as computer hardware is easily appreciated, we must not overlook the larger investment in less tangible information assets - such as data, software, and automated processes.

Information resources are vital assets that require protection. Data, whether stored in central computers accessible through remote terminals, processed locally on personal computers, or generated by word processing systems, is vulnerable to a variety of threats and must be afforded adequate safeguards.

Naval Postgraduate School faculty, staff, and students need to be aware of the value of these resources and the means of protecting them. User awareness through education is the first line of defense in maintaining confidentiality, reliability, availability, and integrity of Naval Postgraduate School information resources.

The Naval Postgraduate School's security policy was developed to assist in the education of faculty, staff, and students in the need for and means of protecting Naval Postgraduate School Information Resources. This document defines the security and data ownership responsibilities of the mission critical computing resources that are maintained and operated by the Naval Postgraduate School. This document should be useful in ongoing departmental security programs for security awareness and training.

### **B. INTRODUCTION**

Continuing availability of information is essential to the operation of Naval Postgraduate School programs. Expanded use of computers and telecommunications has resulted in more accurate, reliable, and faster information processing, with information more readily available to administration, faculty, and staff than ever before. The Naval Postgraduate School has realized increased productivity, in terms of improved delivery of services, enhanced administrative capabilities, and lower operating costs, as a direct result of the growing commitment to use information technology.

Information technology has also brought new administration concerns, challenges, and responsibilities. Information assets must be protected from natural and human hazards. Policies and practices must be established to ensure that hazards are eliminated or their effects minimized.

The focus of information security is on ensuring protection of information and continuation of operations. Providing efficient accessibility to necessary information is the impetus for establishing and maintaining automated information systems. Protecting that information and the surrounding investment is the impetus for establishing an information security program.

Protecting information assets include:

- Physical protection of information processing facilities and equipment.
- Maintenance of application and data integrity.
- Assurance that automated information systems perform their critical functions correctly, in a timely manner, and under adequate controls.
- Protection against unauthorized disclosure of information.
- Assurance of the continued availability of reliable and critical information.

Many program operations that traditionally were manual or partially automated are today fully dependent upon the availability of automated information services to perform and support their daily functions. The interruptions, disruption, or loss of information support services may adversely affect Naval Postgraduate School's ability to administer programs and provide services. The effects of such risks must be eliminated or minimized.

Additionally, information entered, processed, stored, generated, or disseminated by automated information systems must be protected from internal data or programming errors and from misuse by individuals inside or outside the Naval Postgraduate School. Specifically, the information must be protected from unauthorized or accidental modification, destruction, or disclosure. Otherwise, we there is the risk of compromising the integrity of Naval Postgraduate School programs, violating individual rights to privacy, violating copyrights, or facing criminal penalties.

An effective and efficient security management program requires active support and ongoing participation from multiple disciplines and all levels of administration. Responsibilities include identifying vulnerabilities that may affect information assets and implementing cost-effective security practices to minimize or eliminate the effects of the vulnerabilities.

The policies and procedures of this document apply to the mission critical applications and resources operated by the Naval Postgraduate School. These include applications such as the campus computer network (local-area and wide-area); and the computing facilities and workstations purchased for the Naval Postgraduate School's use. In the remainder of this document Information Resources will refer to:

- Network Resources - the Naval Postgraduate School computer network. This does include both Local Area Networks and Wide Area Networks as used by and connected to the Naval Postgraduate School equipment.
- Hardware Resources - all computing resources operated by the Naval Postgraduate School.
- Software Resources - all applications operated by the Naval Postgraduate School or its customers.

## **C. COMPUTER SECURITY POLICY**

### **1. Purpose**

To establish general Naval Postgraduate School (NPS) policy on the security of NPS computing and information systems, consistent with the NPS mission and Department of the Navy/Department of Defense (DoN/DoD) guidelines.

### **2. Policy Scope**

The Computer Security Policy applies to all Automated Information systems owned, operated or administered under the authority of the Superintendent, Naval Postgraduate School (NPS), including the Naval Support Activity Monterey Bay (NSAMB), and the Defense Resource Management Institute (DRMI). It also applies to all DoD/Federal tenant or local commands, activities and agencies, contractors, and all other organizations and individuals that utilize NPS Information Technology resources. It does not apply to classified information systems that fall under the cognizance of the Office of Naval Intelligence.

### **3. Policy Statements**

It is the policy of the Naval Postgraduate School that:

- Any violation of this policy may be enforceable under The Uniform Code of Military Justice or appropriate state or federal statute. (see Annex E)
- Information Resources are valuable assets and unauthorized use, alteration, destruction, or disclosure of these assets is a computer-related crime, punishable under federal laws that are summarized in Annex E, *Computer Security Rules, Regulations, and Laws*.
- Attempting to circumvent security or administrative access controls for Information Resources is a violation of this policy. Assisting someone else or requesting someone else to circumvent security or administrative access controls is a violation of this policy.
- Information Resources may be used only for official purposes.
- Violations of the Computer Security Policy will be reported to the Naval Postgraduate School's Security Manager.
- Violations of the Computer Security Policy that may be violations of state and federal laws will be reported to Naval Investigative Service.
- Persons violating the Computer Security Policy will be subject to appropriate administrative and criminal sanctions.

- All employees will receive the Computer Security Policy Summary Statement. The summary statement is contained in Annex G, *Computer Security Policy Summary Statement*.
- Logon ids and passwords must control access to all Information Resources except for those specific resources identified as being public.
- The logon id owner must change their passwords periodically.
- The logon id owner is responsible for managing their password according to the guidelines specified in Annex B, *Password Management*.
- The legitimate proprietary interests of intellectual property owners will be upheld and supported.
- Information that is classified must be protected from unauthorized access or modification. Data that is essential to critical functions must be protected from loss, contamination, or destruction.
- Classified information shall be accessible only by personnel who are authorized by the owner on a basis of strict "need to know" in the performance of their duties. Data containing any classified information shall be readily identifiable and treated as classified in its entirety.
- When a student, faculty member, or staff member either terminates employment or leaves the institution for a follow-on duty station, their access to Information Resources will be terminated. Annex D, *Personnel Security and Security* contains additional information.
- Microcomputer end-user workstations used in sensitive or critical tasks must have adequate controls to provide continued confidentiality, integrity, and availability of data stored on the system.
- All microcomputer end-user workstations should have virus protection software installed.
- Computer software purchased using DON funds is Naval Postgraduate School System property and shall be protected as such.
- Ownership of computer software developed by faculty, staff, and students is defined in SECNAVINST 5870.3C and Title 15 United States Code 3710c.
- All information processing areas used to house Information Resources supporting critical applications must be protected by physical controls appropriate for the size and complexity of the operations and the criticality or sensitivity of the systems operated at those locations. Physical access to these areas shall be restricted to authorized personnel. Authorized visitors should be supervised and their entry and exit recorded in a log.
- Individuals who believe they have experienced computer generated harassment or illegal discrimination are encouraged to contact the appropriate administrative office to file a complaint. Additional information is provided in Appendix F, *Filing Complaints About Computer Generated Harassment or Discrimination*.
- Internet access to the Naval Postgraduate School Network will be controlled as appropriate under guidelines established by the Information Systems Security Manager in NAVPGSCOL 5230.4B *POLICY ON APPROPRIATE USE OF NAVAL POSTGRADUATE SCHOOL COMPUTING AND INFORMATION SYSTEMS*.

- Network monitoring tools are used to obtain detailed information relating to network performance, security vulnerabilities, and the amount and types of usage. This information can be used to monitor compliance with School policies, including appropriate use. All users should be aware that NPS computer and information systems and networks are subject to monitoring at all times, and that use of these resources implies consent to such monitoring. Consequently, no expectation of privacy should be assumed regarding information transmitted, received, or placed in NPS systems. Violations of the policies defined herein may subject the user to disciplinary action.

#### **4. Policy Administration**

The Computer Security Policy is administered by the Information Systems Security Manager (ISSM) and Code 05. The ISSM has responsibility to:

- Monitor computer security issues
- File regular reports on computer security issues
- Keep users aware of computer security issues
- Monitor compliance with this policy
- Act as primary contact for the Computer Emergency Response Team.
- Chair the Computer Security Committee.
- Further details on responsibilities are covered under Naval Postgraduate School Instruction 5239.1B *NAVAL POSTGRADUATE SCHOOL AUTOMATED INFORMATION SYSTEM SECURITY PROGRAM*

The Computer Security Policy is maintained by the ISSM and the Computer Security Committee. The policy will be reviewed annually and updated as appropriate.

#### **5. Electronic Mail Privacy**

Electronic mail is provided to faculty, staff, and students as part of the Information Resources of Naval Postgraduate School to conduct the business of Naval Postgraduate School and the Naval Postgraduate School System. Electronic mail is intended to be a convenient way for the faculty, staff, and students to communicate with one another and colleagues at other locations. It is not the practice for the Naval Postgraduate School to monitor the contents of electronic mail messages. However, the information in electronic mail files may be subject to disclosure under certain circumstances; for example, requests during legal investigations.

### **ANNEX A - TERMS AND DEFINITIONS**

The following terms that are used in this document are defined to have these meanings:

Computer Security	Those measures, procedures, or controls that provide an acceptable degree of safety of information resources from accidental or intentional disclosure, modification, or destruction.
Data	A representation of facts or concepts in an organized manner in order that it may be stored communicated interpreted

	or processed by automated means.
Generally Accessible Computing Resource	The computing resources of the Naval Postgraduate School available to any faculty, staff, or student at the Naval Postgraduate School.
Information Resources	The computer hardware, software, data files, and networks at Naval Postgraduate School.
LAN	Local Area Networks are connected to Naval Postgraduate School.
Logon ID	A unique identifier used by the computer system to establish user identification.
Critical Information Resources	Those information-processing resources that have been determined to be essential to Naval Postgraduate School's critical mission and functions.
Password	A combination of characters used to authenticate a person's identity to a computer system when associated with a logon id.
Naval Postgraduate School Network	The Ethernet, FDDI, fiber optic, ATM, and the port selector portions of the Naval Postgraduate School campus computing networks.

## **ANNEX B - PASSWORD MANAGEMENT**

Information handled by computer systems must be adequately protected against unauthorized modification, disclosure, or destruction. Effective controls for logical access to information resources minimizes inadvertent employee error and negligence, and reduces opportunities for computer crime. Each user of a mission critical automated system is assigned a unique personal identifier for user identification. User identification is authenticated before the system may grant access to automated information.

### **1. Password Selection**

Passwords are used to authenticate a user's identity and to establish accountability. A password that is easily guessed is a bad password that compromises security and accountability of actions taken by the logon id that represents the user's identity.

Today, computer crackers are extremely sophisticated. Instead of typing each password by hand, crackers use personal computers to make phone calls to try the passwords, automatically re-dialing when they become disconnected. Instead of trying every combination of letters, starting with AAAAAA (or whatever), crackers use hit lists of common passwords such as WIZARD or DEMO. Even a modest home computer with a good password-guessing program can try thousands of passwords in less than a day's

time. Some hit lists used by crackers contain several hundred thousand words. Therefore, any password that anybody might guess to be a password is a bad choice.

What are popular passwords: your name, your spouse's name, or your parents' names. Other bad passwords are these names spelled backwards or followed by a single digit. Short passwords are also bad, because there are fewer of them; they are more easily guessed. Especially bad are "magic words" from computer games, such a XYZZY. Other bad choices include phone numbers, characters from favorite movies or books, local landmark names, favorite drinks, or famous people.

Some rules for choosing a good password are:

- Use both uppercase and lowercase letters if the computer system considers an uppercase letter to be different from a lowercase letter when the password is entered.
- Include digits and punctuation characters as well as letters
- Choose something easily remembered so it doesn't have to be written down.
- Use at least 8 characters. Password security is can potentially be improved slightly greatly by having long passwords.
- It should be easy to type quickly so someone cannot follow what was typed by watching the keyboard.
- Use two short words and combine them with a special character or a number, like ROBOT4ME or EYE-CON.
- Put together an acronym that has special meaning to you, like NOTFSW (None Of This Fancy Stuff Works) or AVPEGCAN (All VAX Programmers Eat Green Cheese At Night).

## **2. Password Handling**

A standard admonishment is "never write down a password." You should not write your password on your desk calendar, on a Post-It label attached to your computer terminal, or on the pullout drawer of your desk.

A password you memorize is more secure than the same password written down, simply because there is less opportunity for other people to learn a memorized password. A password that must be written down in order to be remembered is quite likely a password that is not going to be guessed easily. If you write a password in your wallet, the chances of somebody who steals your wallet using the password to break into your computer account are remote.

If you must write down a password, follow a few precautions:

- Do not identify the password as being a password.
- Do not check the box when prompted by an application to "remember my password for me."
- Do not include the name of the account or the phone number of the computer on the same piece of paper.
- Do not attach the password to a terminal, keyboard, or any part of a computer.

- Mix in some "noise" characters or scramble the written version of the password in a way that you remember, but make the written version different from the real password.
- Never record a password on-line and never send a password to another person via electronic mail.

## **ANNEX C - DISASTER RECOVERY**

It is prudent and required by the Department of the Navy to anticipate and prepare for the loss of information processing capabilities. The plans and actions to recover from losses range from routine backup of data and software in the event of minor losses or temporary outages, to comprehensive disaster recovery planning in the preparation for catastrophic losses of information resources.

### **1. Data Backup**

The backup procedures on the servers are designed to protect against data losses caused by hardware failures and other disasters. The frequency and timing of these backups may not provide sufficient protection to meet end-user requirements for data backup. Therefore, it is strongly recommended that end-users include a data backup step in their information processing procedures, and not to depend on single backup procedure to provide all protection.

Data and software essential to the continued operation of critical department functions must be backed up. The security controls over the backup resources must be as stringent as the protection required of the primary resources.

### **2. Contingency Planning**

Contingency plans, or disaster control plans, specify actions management have approved in advanced to achieve each of three objectives: to identify and respond to disasters; to protect personnel and systems; and to limit damage. The backup plan specifies how to accomplish critical portions of the mission in the absence of a critical resource such as computers. The recovery plan directs recovery of full mission capability.

## **ANNEX D - PERSONNEL SECURITY AND SECURITY AWARENESS**

In any organization, people are the greatest asset in maintaining an effective level of security. At the same time, people represent the greatest threats to information security. No security program can be effective without maintaining employee awareness and motivation.

### **1. Permanent Personnel and Student Requirements**

All permanent personnel and students are responsible for systems security to the degree that their responsibilities require the use of information and associated systems. Fulfillment of security responsibilities is mandatory and violations of security requirements may be cause for disciplinary action, up to and including dismissal, civil penalties, and criminal penalties.



## ANNEX E - COMPUTER SECURITY RULES, REGULATIONS, AND LAWS

There are several NPS Instructions and a number of state and federal laws that affect the security of information processing resources, computer systems, computer software, and data files. The following summaries are provided for the reader to review:

- Naval Postgraduate School Instruction 5230.4B *POLICY ON APPROPRIATE USE OF NAVAL POSTGRADUATE SCHOOL COMPUTING AND INFORMATION SYSTEMS*. Regulations concerning computer security and use of Naval Postgraduate School computing resources by students, faculty and staff.
- Naval Postgraduate School Instruction 5239.1B *NAVAL POSTGRADUATE SCHOOL AUTOMATED INFORMATION SYSTEM SECURITY PROGRAM*
  1. Regulations concerning computer security and policy, standards, and guidelines for Information Resources Security and Risk
  2. Detailed description of individual responsibilities pertaining to the security of NPS computer and informational resources
  3. To provide a framework for the formal security accreditation of all NPS information systems
  4. To promote and encourage the consideration of security issues in the Life Cycle Management (LCM) process
  5. Guidelines pertaining to Security Training
- NPS Memorandum dated 1 June 1995 *Interim Policy on Establishment and Operation of Internet Open, Anonymous Information Servers and Services*. This Memo establishes interim policy on establishment and operation of Internet open, Anonymous Information Servers and services, such as World Wide Web (http), Anonymous FTP, etc.
- OPNAV INSTRUCTION 5239.1B *NAVY INFORMATION ASSURANCE (AI) PROGRAM*. This establishes policies and procedures for the U.S. Navy's Information Assurance Program.
- SECNAV INSTRUCTION 5239.3 *DEPARTMENT OF THE NAVY INFORMATION SYSTEMS SECURITY (INFOSEC) PROGRAM*. Establishes Department of Navy policy for the INFOSEC Program within the Information Warfare discipline and to define the organizational responsibilities for implementation of the security disciplines of Communications Security, Computer Security and Emanations Security.
- Federal Copyright Law. Recognizes that all intellectual works are automatically covered by copyright. The owner of a copyright holds the exclusive right to reproduce and distribute the work.
- Computer Fraud and Abuse Act of 1986. Makes it a crime to access a computer to obtain restricted information without authorization; to alter, damage, or destroy

information on a government computer; and to traffic in passwords or similar information used to gain unauthorized access to a government computer.

- Electronic Communications Privacy Act of 1986. Prohibits the interception or disclosure of electronic communication and defines those situations in which disclosure is legal.

## **ANNEX F - FILING COMPLAINTS ABOUT COMPUTER GENERATED HARASSMENT OR DISCRIMINATION**

Faculty, staff, or students who allege harassment or discrimination as a result of words or images generated or transmitted by an individual using Naval Postgraduate School System computing resources may file a complaint against that individual in accordance with the Department of the Navy Procedures for Sexual Harassment Complaints and Equal Opportunity Violations

If the complaint is against a student, the complaint is filed with: The student's chain of command.

If the complaint is against a faculty member, the complaint is filed with:  
Department Chairmen

If the complaint is against a staff member, the complaint is filed with: Human Resources Department

## **APPENDIX G - COMPUTER SECURITY POLICY SUMMARY STATEMENT**

### **Summary Statement**

Naval Postgraduate School has developed a comprehensive computer security policy statement. This summary statement presents an overview and the key points of the Naval Postgraduate School Computer Security Policy.

The Information Resources at Naval Postgraduate School are extensive and are readily available to authorized users. This availability of computer hardware, software, and database resources brings with it the responsibility to protect those resources from unauthorized access, unauthorized use, or inappropriate use. During the past several years, much has been written about viruses, worms, and hackers. While these are very real and present dangers, we must also be aware of the dangers from careless activities regarding Information Resources at Naval Postgraduate School, particularly in the network environment.

The Naval Postgraduate School Computer Security Policy is available electronically at [www.nps.navy.mil/secpolicy](http://www.nps.navy.mil/secpolicy).

The main items of the Computer Security Policy are:

Each user of an Information Resource must be responsible for certain key aspects of security, which include:

- The Appropriate handling of passwords and password procedures
- Using resources, hardware and software, in accordance with the owner's guidelines
- Taking precautions with regard to viruses
- Following the prescribed procedures for access and use of data
- Adhering to copyright policies

Naval Postgraduate School has instituted certain computer security measures designed to protect the integrity of Information Resources. Any attempt to circumvent these procedures may be a violation of Naval Postgraduate School policies, rules, and regulations, and state and federal statutes.

Virus protection software should be installed on all microcomputer end-user workstations.

All users of Information Resources acknowledge their reading and understanding of computer security issues each time they logon to a Naval Postgraduate School computer system.

THIS PAGE INTENTIONALLY LEFT BLANK

## **APPENDIX D: GROUP POLICY SETTINGS**

### **INTRODUCTION**

This Appendix is a listing of all the Group Policy Settings available in Windows 2000 Server edition. All the settings are directly related to registry entries and can be manipulated through the Group Policy Editor Microsoft Management console. This appendix initially contains a summary of all the configuration categories, then a listing of all the individual settings. The recommended method to navigate through this document is to find the category/sub-category of the setting, then go back to the table of contents to find the page number of the sub-category. NOTE: If this is the electronic version, the page containing the sub-category can be accessed by moving the curser over the page number in the Table of Contents and then left clicking the pointing device.

## SUMMARY TABLE OF POLICY SETTINGS

### Computer Configuration

#### Software Settings

#### Software Installation

#### Windows Settings

#### Scripts (Startup / Shutdown)

*Startup*

*Shutdown*

#### Security Settings

#### Account Policies

##### Password Policy

*Enforce password history*

*Maximum password age*

*Minimum password length*

*Minimum password age*

*Password must meet complexity requirements*

*Store password using reversible encryption for all users in the domain*

##### Account Lockout Policy

*Account lockout duration*

*Account lockout threshold*

*Reset lockout counter after*

##### Kerberos Policy

*Enforce user logon restrictions*

*Maximum lifetime for service ticket*

*Maximum lifetime for user ticket*

*Maximum lifetime for user ticket renewal*

*Maximum tolerance for computer clock synchronization*

#### Local Policies

##### Audit Policy

*Audit account logon events*

*Audit account management*

*Audit directory service access*

*Audit logon events*

*Audit object access*

*Audit policy change*

*Audit privilege use*

*Audit process tracking*

*Audit system events*

##### User Rights Assignment

*Access this computer from the network*

*Act as part of the operating system*

- Add workstations to the domain*
- Backup files and directories*
- Bypass traverse checking*
- Change the system time*
- Create a pagefile*
- Create a token object*
- Create permanent shared objects*
- Debug programs*
- Deny access to this computer from the network*
- Deny logon as a batch job*
- Deny logon as a service*
- Deny logon locally*
- Enable computer and user accounts to be trusted for delegation*
- Force shutdown from a remote system*
- Generate security audits*
- Increase quotas*
- Increase scheduling priority*
- Load and unload device drivers*
- Lock pages in memory*
- Log on as a batch job*
- Log on as a service*
- Log on locally*
- Manage audit and security log*
- Modify firmware environment values*
- Profile single process*
- Profile system performance*
- Remove computer from docking station*
- Replace a process level token*
- Restore files and directories*
- Shut down the system*
- Synchronize directory service data*
- Take ownership of files and other objects*

## **Security Options**

- Additional restrictions for anonymous connections*
- Do not allow enumeration of SAM accounts and shares.*
- Allow server operators to schedule tasks (domain controllers only)*
- Allow system to shut down without having to log on*
- Allowed to reject removable NTFS media*

*Amount of idle time required before disconnecting session*

*Audit the access of global system objects*

*Audit use of backup and restore privilege*

*Automatically log off users when log on time expires*

*Automatically log off users when log on time expires (local)*

*Clear virtual memory pagefile when system shuts down*

*Digitally sign client communications (always)*

*Digitally sign client communications (when possible)*

*Digitally sign server communications (always)*

*Digitally sign server communications (when possible)*

*Disable CTRL+ALT+DEL requirement for logon*

*Do not display last user name in logon screen*

*LAN Manager Authentication level*

*Message text for users attempting to logon*

*Message title for users attempting to logon*

*Number of previous logons to cache (in case domain controller is not available)*

*Prevent system maintenance of computer account password*

*Prevent users from installing print drivers*

*Prompt user to change password before expiration*

*Recovery console: Allow automatic administrative logon*

*Recovery console: Allow floppy copy and access to all drives and all folders*

*Rename guest account*

*Restrict CD-Rom access to locally logged on user only*

*Restrict floppy access to locally logged on user only*

*Secure channel: Digitally encrypt or sign secure channel data (always)*

*Secure channel: Digitally encrypt secure channel data (when possible)*



*Secure channel: Digitally sign secure channel data (when possible)*

*Secure channel: Require strong (Windows 2000 or later) session key*

*Secure system partition (for RISC Platforms only)*

*Shut down system immediately if unable to log security audits*

*Smart card removal behavior*

*Strengthen default permissions of global system objects (e.g. Symbolic links)*

*Unsigned driver installation behavior*

## **Event Logs**

### **Settings for Event Logs**

*Maximum application log size*

*Maximum security log size*

*Maximum system log size*

*Restrict guest access to application log*

*Restrict guest access to security log*

*Restrict guest access to system log*

*Retain application log*

*Retain system log*

*Retain security log*

*Retention method for application log*

*Retention method for security log*

*Retention method for system log*

*Shut down the computer when the security audit log is full*

## **Restricted Groups**

## **System Services**

## **Registry**

## **File System**

## **Public Key Policies**

## **IP Security Policies on Active Directory**

## **Administrative Templates**

### **Windows Components**

#### **Net Meeting**

*Disable remote desktop sharing*

#### **Internet Explorer**

*Security Zones: Use only machine settings*

*Security Zones: Do not allow users to change policies*

*Security Zones: Do not allow users to add/delete sites*

*Make proxy settings per machine*

*Disable automatic install of Internet Explorer components*

*Disable periodic check for IE software updates*

*Disable software update shell notifications on program launch*

*Disable showing the splash screen*

### **Task Scheduler**

*Hide property pages*

*Prevent task run or end*

*Disable drag and drop*

*Disable new task creation*

*Disable task deletion*

*Disable advanced menu*

*Prohibit browse*

### **Windows Installer**

*Disable windows installer*

*Always install with elevated privileges*

*Disable rollback*

*Disable browse dialog box for new source*

*Disable patching*

*Disable IE security prompt for windows installer script*

*Enable user control over installs*

*Enable user to browse the source while elevated*

*Enable user to use media source while elevated*

*Enable user to patch elevated products*

*Allow admin to install from terminal services session*

*Cache transforms in secure location on workstation*

*Logging*

### **System**

*Remove security option from start menu*

*Remove disconnect item from start menu*

*Disable Boot / Shutdown / Logon / Logoff status messages*

*Verbose vs. normal status messages*

*Display Autoplay*

*Don't display welcome screen at logon*

*Run these programs at user logon*

*Disable the run once list*

*Disable legacy run list*

*Do not automatically encrypt files moved to encrypted folders*

*Download missing COM components*

### **Logon**

*Run logon scripts synchronously*

*Run startup scripts asynchronously*  
*Run startup scripts visible*  
*Run Shutdown scripts visible*  
*Maximum wait time for group policy scripts*  
*Delete cached copies of roaming profiles*  
*Do not detect slow network connections*  
*Slow network connection time out for user profiles*  
*Wait for remote user profile*  
*Prompt user when slow link is detected*  
*Timeout for dialog boxes*  
*Log users off when roaming profile fails*  
*Maximum retries to unload and update user profile*

### **Disk Quotas**

*Enable disk quotas*  
*Enforce disk quota limit*  
*Default quota limit and warning level*  
*Log event when quota limit exceeded*  
*Log event when quota warning level exceeded*  
*Apply policy to removable media*

### **DNS Client**

*Primary DNS suffix*

### **Group Policies**

*Disable background refresh of group policy*  
*Apply group policy for computers asynchronously during startup*  
*Apply group policy for users asynchronously during logon*  
*Group policy refresh interval for computers*  
*Group policy refresh interval for domain controllers*  
*User group policy loopback processing mode*  
*Group policy slow link detection*  
*Registry policy processing*  
*IE maintenance policy processing*  
*Software installation policy processing*  
*Folder redirection policy processing*  
*Scripts policy processing*  
*Security policy processing*  
*IP security policy processing*  
*EFS recovery policy processing*  
*Disk quota policy processing*

### **Windows File Protection**

*Set Windows file protection scanning*

*Hide the file scan process window*  
*Limit Windows file protection cache size*  
*Specify Windows file protection cache location*

## **Network**

### **Offline Files**

*Enabled*  
*Disable user configuration of offline files*  
*Synchronize all offline files before logging off*  
*Default cache size*  
*Action on server disconnect*  
*Non-default server disconnect actions*  
*Disable “Make available offline”*  
*Files not cached*  
*Administratively assigned offline files*  
*Disable reminder balloons*  
*Reminder balloon frequency*  
*Initial reminder balloon lifetime*  
*Reminder balloon lifetime*  
*At logoff, delete local copy of user’s offline files*  
*Event logging level*  
*Subfolders always available offline*

### **Network and Dial-up Connections**

*Allow configuration of connection sharing*

## **Printers**

*Allow printers to be published*  
*Automatically new printers in active directory*  
*Allow pruning of published printers*  
*Printer browsing*  
*Prune printers that are not automatically republished*  
*Directory pruning interval*  
*Directory pruning retry*  
*Directory pruning priority*  
*Check published state*  
*Web based printing*  
*Custom support URL in the printer’s folders left pane*  
*Computer location*  
*Pre-populate printer search location text*

## **User Configuration**

### **Software Settings**

#### **Software installation**

### **Windows Settings**

#### **IE maintenance**

#### **Browser user interface**

#### **Browser Title**

- Animated Bitmaps
  - Custom Logo
  - Browser Toolbar buttons
- Connection
  - Connection Settings
  - Automated Browser configuration
  - Proxy settings
  - User agent strings
- URLs
  - Favorites and Links
  - Important URLs
  - Channels
- Security
  - Security Zones and content ratings
  - Authenticode settings
- Programs
  - Programs
- Scripts
  - Logon*
  - Logoff*
- Security Settings
  - Public key policies
    - Enterprise trust
  - Remote Installation Service
    - Choice options
- Folder Redirection
  - Application Data
  - Desktop
  - My Documents
    - My Pictures
  - Start Menu
- Administrative Templates
  - Windows Components
    - Netmeeting
      - Enable automatic configuration*
      - Disable directory services*
      - Prevent adding directory servers*
      - Prevent viewing web directory*
      - Set the intranet support page*
      - Set call security option*
      - Prevent changing call placement method*
      - Prevent automatic acceptance of calls*
      - Prevent sending files*
      - Prevent receiving files*
      - Limit the size of sent files*

*Disable chat*

*Disable Netmeeting 2.X whiteboard*

*Disable whiteboard*

### **Application Sharing**

#### **(i) Disable Application sharing**

*Prevent sharing*

*Prevent desktop sharing*

*Prevent sharing command prompts*

*Prevent sharing explorer windows*

*Prevent control*

*Prevent application sharing in true color*

### **Audio and Video**

#### **(ii) Limit the bandwidth of audio and video**

*Disable audio*

*Disable full duplex audio*

*Prevent changing direct sound audio settings*

*Prevent sending video*

*Prevent receiving video*

### **Options Page**

*Hide the general page*

*Disable the advanced calling button*

*Hide the security page*

*Hide the audio page*

*Hide the video page*

### **Internet Explorer**

*Search: Disable search customization*

*Search: Disable find files via F3 within browser*

*Disable external branding of IE*

*Disable importing and exporting of favorites*

*Disable changing advanced page settings*

*Disable changing home page settings*

*Use automatic detection for dial-up connections*

*Disable caching of auto-proxy scripts*

*Display error message on proxy script download failure*

*Disable changing temporary internet files settings*

*Disable changing history settings*

*Disable changing color settings*

*Disable changing link color settings*

*Disable changing font color settings*

*Disable changing language settings*

*Disable changing accessibility settings*  
*Disable internet connection wizard*  
*Disable connection settings*  
*Disable changing proxy settings*  
*Disable changing automatic configuration settings*  
*Disable changing ratings settings*  
*Disable changing certificate settings*  
*Disable changing profile assistant settings*  
*Disable autocomplete for forms*  
*Do not allow autocomplete to save passwords*  
*Disable changing messaging settings*  
*Disable changing calendar and contact settings*  
*Disable the reset web settings feature*  
*Disable changing default browser check*  
*Identity manager: Prevent users from using*

#### *Identities*

#### **Internet Control Panel**

*Disable the general page*  
*Disable the security page*  
*Disable the content page*  
*Disable the connections page*  
*Disable the programs page*  
*Disable the advanced page*

#### **Offline Pages**

*Disable adding channels*  
*Disable removing channels*  
*Disable adding schedules for offline pages*  
*Disable editing schedules for offline pages*  
*Disable removing schedules for offline*  
*pages*  
*Disable offline pages hit logging*  
*Disable all scheduled offline pages*  
*Disable channel user interface completely*  
*Disable downloading of site subscription*  
*content*  
*Disable editing and scheduling of scheduled*  
*groups*  
*Subscription limit*

#### **Browser Menus**

*File menu: Disable Save as... menu option*  
*File menu: Disable New menu option*  
*File menu: Disable Open menu option*  
*File menu: Disable Save as Web Page*  
*Complete*

*File menu: Disable closing browser and explorer windows*

*View menu: Disable Full Screen menu option*

*Hide Favorites menu*

*Tool menu: Disable Internet Options... menu option*

*Help menu: Remove "Tip of the Day" menu option*

*Help menu: Remove "For Netscape Users" menu option*

*Help menu: Remove Tour menu option*

*Help menu: Remove "Send feedback" menu option*

*Disable context menu*

*Disable open in new window menu option*

*Disable save this program to disk option*

### **Toolbars**

*Disable customizing browser toolbar buttons*

*Disable customizing browser tool bars*

*Configure toolbar buttons*

### **Persistence Behavior**

*File size limits for local machine zones*

*File size limits for Intranet zone*

*File size limits for trusted sites zone*

*File size limits for Internet zone*

*File size limits for restricted sites zone*

### **Administrator Approval Controls**

*Media Player*

*Menu controls*

*Microsoft agent*

*Microsoft chat*

*Microsoft survey control*

*Shockwave flash*

*Netshow file transfer control*

*DHTML edit control*

*Microsoft scriptlet component*

*Carpoint*

*Investor*

*MSNBC*

## **Windows Explorer**

### **Common Open File Dialog**

*Hide the common dialog places bar*

*Hide the common dialog back button*



- Hide the dropdown list of recent files*
- Enable classic shell*
- Removes the folder options menu item from the tools menu*
- Remove file menu from windows explorer*
- Remove “Map network drive” and “Disconnect network drive”*
- Remove search button for windows explorer*
- Disable window explorer’s default context menu*
- Hides the manage item on the windows explorer context menu*
- Only allow approved shell extensions*
- Do not track shell shortcuts during roaming*
- Hide these specified drives in My computer*
- Prevents access to drives from My computer*
- Hide hardware tab*
- Disable UI to change menu animation settings*
- Disable UI to change keyboard navigation indicator settings*
- Disable DFS tab*
- No “Computers near me” in My network place*
- No “Entire network” in My network place*
- Maximum number of recent documents*
- Do not request alternate credentials*
- Request credentials for network installations*

### **Microsoft Management Console**

- Restrict the user from entering the author mode*
- Restrict the users to the explicitly permitted list of snap-ins*

#### **Restricted/Permitted Snap-ins**

- Active directory users and computers*
- Active directory sites and services*
- Certificates*
- Component Services*
- Computer management*
- Device manager*
- Disk Management*
- Disk Defragmenter*
- Distributed File System*

#### **(iii) Event viewer**

- FAX service*
- Indexing service*
- Internet Authentication service*
- Internet information service*

*IP security*  
*Local users and groups*  
*Performance logs and alerts*  
*QoS admission control*  
*Removable storage management*  
*Routing and remote access*  
*Security Configuration and analysis*  
*Security templates*  
*Services*  
*Shared folders*  
*System information*  
*Telephony*  
*Terminal services configuration*  
*VMI control*

**Extension Snap-ins**

*Apple Talk Routing*  
*Certification Authority*  
*Connection sharing (NAT)*  
*DCOM configuration extension*  
*Device manager*  
*DHCP relay management*  
*Event viewer*  
*IAS Logging*  
*IGMP routing*  
*IPX routing*  
*IPX RIP routing*  
*IPX SAP routing*  
*Logical and mapped drives*  
*OSPF routing*  
*Public Key policies*  
*RAS dial-in*  
*Remote Access*  
*Removable storage*  
*RIP routing*  
*Routing*  
*Send console message*  
*Services dependencies*  
*SMTP Protocol*  
*SNMP*  
*System properties*

**Group Policy**

*Group policy snap-in*  
*Group policy tab for active directory*

*tools*

*Administrative templates*  
*(Computers)*

*Administrative templates (Users)*  
*Folder Redirection*  
*Internet Explorer Maintenance*  
*Remote installation service*  
*Scripts (logon/logoff)*  
*Scripts (startup/shutdown)*  
*Security settings*  
*Software installation (Computers)*  
*Software installation (Users)*

**Task Scheduler**

*Hide property pages*  
*Prevent task run or end*  
*Disable Drag-and-drop*  
*Disable new task creation*  
*Disable task deletion*  
*Disable advanced menu*  
*Prohibit browse*

**Windows Installer**

*Always install with elevated privileges*  
*Search order*  
*Disable rollback*  
*Disable media source for any install*

**Start menu and taskbar**

*Remove user's folder from the start menu*  
*Disable and remove links to windows update*  
*Remove common programs group from start menu*  
*Remove documents menu from start menu*  
*Disable programs on setting menu*  
*Remove networks and dial-up connections from start menu*  
*Remove favorites menu from start menu*  
*Remove search menu from start menu*  
*Remove help menu from start menu*  
*Remove run menu from start menu*  
*Add logoff to start menu*  
*Disable logoff on the start menu*  
*Disable and remove the shutdown command*  
*Disable drag-and-drop context menus from the start menu*  
*Disable changes to taskbar and start menu settings*  
*Disable context menus for the taskbar*  
*Do not keep history of recently opened document*  
*Clear history of recently opened documents on exit*  
*Disable personalized menus*  
*Disable user tracking*

*Add “Run in separate memory space” check box to run dialog box*

*Do not use the search based method when resolving shell shortcuts*

*Do not use the tracking based method when resolving shell shortcuts*

*Gray unavailable windows installer programs start menu shortcuts*

## **Desktop**

*Hide all icons on Desktop*

*Remove my documents icon from desktop*

*Remove my documents icon from start menu*

*Hide my network places icon on desktop*

*Hide my Internet Explorer icon on desktop*

*Do not add shares of recently opened document to My network place*

*Prohibit users from changing My Documents path*

*Disable adding, dragging, dropping, and closing the taskbar’s toolbar*

*Disable adjusting taskbar’s toolbar*

*Don’t save settings at exit*

## **Active desktop**

*Enable active desktop*

*Disable active desktop*

*Disable all items*

*Prohibit changes*

*Prohibit adding items*

*Prohibit deleting items*

*Prohibit editing items*

*Prohibit closing items*

*Add/delete items*

*Active desktop wallpaper*

*Allow only bitmapped wallpaper*

## **Active directory**

*Maximum size of active directory searches*

*Enable filter to find dialog box*

*Hide active directory folder*

## **Control panel**

*Disable Control Panel*

*Hide specified control panel applets*

*Show only specified control panel applets*

## **Add/Remove programs**

*Disable Add/Remove programs*

*Hide change or remove program page*

*Hide add new programs page*

*Hide add remove windows components page*  
*Hide the “Add a program from CD-ROM or floppy disk” option*  
*Hide the “Add the program from Microsoft” option*  
*Hide the “Add program from your network” option*  
*Go directly to the components wizard*  
*Disable support information*  
*Specify default category for Add new programs*

### **Display**

*Disable display in control panel*  
*Hide background tab*  
*Disable changing wallpaper*  
*Hide appearance tab*  
*Hide settings tab*  
*Hide screen saver tab*  
*No screen saver*  
*Screen saver executable name*  
*Password protect the screen saver*

### **Printers**

*Disable deletion of printers*  
*Disable addition of printers*  
*Browse the network to find printers*  
*Default active directory path when searching for printers*  
*Browse a common web site to find printers*

### **Regional options**

*Restrict selection of Windows 2000 menus and dialogs language*

## **Network**

### **Offline files**

*Disable user configuration of offline files*  
*Synchronize all offline files before logging off*  
*Action of server disconnect*  
*Non-default server disconnect actions*  
*Disable “make available offline”*  
*Disable use of offline files folder*  
*Administratively assign offline files*  
*Disable reminder balloons*  
*Reminder balloon frequency*  
*Initial reminder balloon lifetime*  
*Reminder balloon lifetime*  
*Event logging level*

### **Network and dialup connections**

*Disable deletion of RAS connections*

*Enable deletion of RAS connections available to all users*

*Enable connecting and disconnecting a RAS connection*

*Enable connecting and disconnecting a LAN connection*

*Enable access to properties of a LAN connection*

*Allow access to current user's RAS connection properties*

*Enable access to properties of RAS connections available to all users*

*Enable renaming of connections, if supported*

*Enable renaming of RAS connections belonging to the current user*

*Enable adding and removing components for a RAS or a LAN connection*

*Allow connection components to be enabled or disabled*

*Enable access to properties of components of a LAN connection*

*Enable access to properties of components of a RAS connection*

*Disable and enable the network connection wizard*

*Enable status statistics for an active connection*

*Enable the dial-up preferences item on the advanced menu*

*Enable the advanced settings item on the advanced menu*

*Allow configuration of connection sharing*

*Allow TCP/IP advanced configuration*

## **System**

*Don't display welcome screen at logon*

*Century interpretation for year 2000*

*Code signing for device drivers*

*Custom user interface*

*Disable the command prompt*

*Disable registry editing tools*

*Run only allowed windows applications*

*Don't run specified windows applications*

*Disable autoplay*

*Download missing COM components*

### **Logon/Logoff**

*Disable task manager*

*Disable lock computer*

*Disable change password*  
*Disable logoff*  
*Run logon scripts synchronously*  
*Run legacy logon scripts hidden*  
*Run logon scripts visible*  
*Run logoff scripts visible*  
*Connect home directory to root of the share*  
*Limit profile size*  
*Exclude directories in roaming profile*  
*Run these programs at user logon*  
*Disable the run once list*  
*Disable legacy run list*

**Group Policy**

*Group policy refresh interval for users*  
*Group policy slow link detection*  
*Group policy domain controller selection*  
*Create new group policy object links disable by default*  
*Enforce show policies only*  
*Disable automatic update of ADM files*







## COMPUTER CONFIGURATION

### SOFTWARE SETTINGS

#### Software Installation

### WINDOWS SETTINGS

#### Scripts (Startup / Shutdown)

*Startup*

*Shutdown*

#### Security Settings

##### *Account Policies*

(2)

Password Policy

##### ***Enforce password history***

Determines the number of unique new passwords that have to be associated with a user account before an old password can be reused. The value must be between 0 and 24 passwords.

By default, this setting is defined in the Default Domain Group Policy object (GPO) and in the local security policy of workstations and servers with a value of 1.

The intent of this policy is to enable administrators to enhance security by ensuring that old passwords are not continually reused (Microsoft Developer's Network, 2000).

##### ***Maximum password age***

Determines the period of time (in days) that a password can be used before the system requires the user to change it. You can set passwords to expire after a number of days between 1 and 999, or you can specify that passwords never expire by setting the number of days to 0.

By default, this setting is defined in the Default Domain Group Policy object (GPO) and in the local security policy of workstations and servers with a value of 42 (Microsoft Developer's Network, 2000).

##### ***Minimum password length***

Determines the period of time (in days) that a password must be used before the user can change it. You can set values between 1 and 999 days, or you can allow changes immediately by setting the number of days to 0.

By default, this setting is defined in the Default Domain GPO and in the local security policy of workstations and servers with a value of 0, which allows passwords to be changed immediately.

Note: The minimum password age must be less than the Maximum password age.

Configure the minimum password age to be more than 0 if you would like to have entered a value for Enforce password history to be effective. Without a minimum password age, the user can repeatedly cycle through passwords until they get to an old favorite. The reason the default settings do not adhere to this recommendation is to support the scenario where an administrator specifies a password for the user and requires that user to change the administrator-defined password when the user logs on. If password history were set to 0, then the user would not have to pick a new password. Thus, password history is set to 1 by default to handle this specific case (Microsoft Developer's Network, 2000).

### ***Minimum password age***

Determines the least number of characters a user account's password may contain. You can set values between 1 and 14 characters, or you can establish that no password is required by setting the number of characters to 0.

By default, this setting is defined in the Default Domain Group Policy object (GPO) and in the local security policy of workstations and servers with a value of 0 (Microsoft Developer's Network, 2000).

### ***Password must meet complexity requirements***

Determines whether passwords must meet complexity requirements.

By default, this setting is disabled in the Default Domain Group Policy object (GPO) and in the local security policy of workstations and servers.

If this policy is enabled, then passwords must meet the minimum requirements described in the Notes section.

Notes: The default password filter (passfilt.dll) included with Windows 2000 requires that a password:

- Does not contain all or part of the user's account name

- Is at least six characters in length

- Contains characters from three of the following four categories:

  - English upper case characters (A..Z)

  - English lower case characters (a..z)

  - Base 10 digits (0..9)

  - Non-alphanumeric (For example, !,\$#,%)

- Complexity requirements are enforced upon password change or creation.

To create custom password filters, refer to the Microsoft Platform Software Development Kit and the Microsoft Knowledge Base (Microsoft Developer's Network, 2000).

### ***Store password using reversible encryption***

#### ***for all users in the domain***

Determines whether Windows 2000 will store passwords using reversible encryption.

The intent of this policy is to provide support for applications that use protocols that require knowledge of the user password for authentication purposes. Storing passwords using reversible encryption is essentially the same as storing clear-text versions of the passwords. For this reason, this policy should never be enabled unless application requirements outweigh the need to protect password information.

By default, this setting is disabled in the Default Domain Group Policy object (GPO) and in the local security policy of workstations and servers (Microsoft Developer's Network, 2000).

### ***User must log on to change password***

Determines whether users have to log on before they can change their password.

By default, this setting is disabled in the Default Domain Group Policy object (GPO) and in the local security policy of workstations and servers.

If this policy is enabled, then users have to log on before changing their password. Thus, if a

user's password expires, the user will not be able to change the expired password, but must instead have an administrator reset the password (Microsoft Developer's Network, 2000).

(3) Account Lockout Policy

***Account lockout duration***

Determines the number of failed logon attempts that will cause a user account to be locked out. A locked out account cannot be used until it is reset by an administrator or the account lockout duration has expired. You can set values between 1 and 999 failed logon attempts, or you can specify that the account will never be locked out by setting the value to 0.

By default, this setting is disabled in the Default Domain Group Policy object (GPO) and in the local security policy of workstations and servers.

Note: Failed password attempts against workstations or member servers that have been locked using either CTRL+ALT+DELETE or password-protected screen savers do not count as failed logon attempts (Microsoft Developer's Network, 2000).

***Account lockout threshold***

Determines the number of minutes a locked out account remains locked out before automatically becoming unlocked. The range is 1 to 99999 minutes. You can specify that the account will be locked out until an administrator explicitly unlocks it by setting the value to 0.

By default, this policy is not defined, since it only has meaning when an Account lockout threshold is specified.

If an Account lockout threshold is defined, then the Account lockout duration must be greater than or equal to the reset time (Microsoft Developer's Network, 2000).

***Reset lockout counter after***

Determines the number of minutes that must elapse after a failed logon attempt before the bad logon attempt counter is reset to 0 bad logons. The range is 1 to 99999 minutes.

By default, this policy is not defined, since it only has meaning when an Account lockout threshold is specified.

If an Account lockout threshold is defined, then this reset time must be less than or equal to the Account lockout duration.

(4) Kerberos Policy

***Enforce user logon restrictions***

Determines whether the Kerberos Key Distribution Center (KDC) validates every request for a session ticket against the user rights policy of the target computer. Validation of each request for a session ticket is optional because the extra step takes time and may slow network access to services.

By default, this setting is enabled in the Default Domain Group Policy object (GPO).

When this policy is enabled, the user requesting the session ticket must have the right to Log on locally (if the requested service is running on the same machine) or the right to Access this computer from the network (if the requested service is on a remote machine) in order to receive a session ticket. If the policy is disabled, this check is not performed (Microsoft Developer's Network, 2000).

***Maximum lifetime for service ticket***

Determines the maximum amount of time (in minutes) that a granted session ticket can be used to access a particular service. The setting must be greater than ten minutes and less than or equal to the setting for Maximum lifetime for user ticket.

By default, this value is set to 600 minutes (10 hours) in the Default Domain Group Policy object (GPO).

Note: If a client presents an expired session ticket when requesting a connection to a server, the server returns an error message. The client must request a new session ticket from the Kerberos Key Distribution Center (KDC). Once a connection is authenticated, however, it no longer matters whether the session ticket remains valid. Session tickets are used only to authenticate new connections with servers. Ongoing operations are not interrupted if the session ticket used to

authenticate the connection expires during the connection (Microsoft Developer's Network, 2000).

***Maximum lifetime for user ticket***

Determines the maximum amount of time (in hours) that a user's ticket-granting ticket (TGT) may be used. When a user's TGT expires, a new one must be requested or the existing one must be "renewed."

By default, this setting is set to 10 hours in the Default Domain Group Policy object (GPO) (Microsoft Developer's Network, 2000).

***Maximum lifetime for user ticket renewal***

Determines the period of time (in days) during which a user's ticket-granting ticket (TGT) may be renewed.

By default, this setting is set to 7 days in the Default Domain Group Policy object (GPO) (Microsoft Developer's Network, 2000).

***Maximum tolerance for computer clock synchronization***

Determines the maximum time difference (in minutes) that Kerberos will tolerate between the time on a client's clock and the time on a server's clock while still considering the two clocks synchronous.

In order to prevent "replay attacks," Kerberos uses timestamps as part of its protocol definition. For timestamps to work properly, the clocks of the client and the server need to be in synch as much as possible. In other words, both computers need to be set to the same time and date. Because the clocks of two computers are often out of synch, administrators can use this policy to establish the maximum acceptable difference to Kerberos between a client's clock and server's clock. If the difference between a client's clock and the server's clock is less than the maximum time difference specified in this policy, any timestamp used in a session between the two computers will be considered authentic.

By default, this value is set to 5 minutes in the Default Domain Group Policy object (GPO) (Microsoft Developer's Network, 2000).

***Audit account logon events***

Determines whether to audit each instance of a user logging on or logging off of another computer where this computer was used to validate the account.

For domain controllers, this policy is defined in the Default Domain Controllers Group Policy object (GPO). The default setting is **No auditing**.

If you define this policy setting, you can specify whether to audit successes, audit failures, or not to audit the event type at all. Success audits generate an audit entry when account logon occurs successfully. Failure audits generate an audit entry when an attempted occurrence of the account logon fails. You can select No auditing by defining the policy setting and unchecking Success and Failure.

As an example, if success auditing for account logon events is enabled on a domain controller, then an entry is logged for each user validated against that domain controller even though the user is actually logging on to a workstation that is joined to the domain (Microsoft Developer's Network, 2000).

***Audit account management***

Determines whether to audit each event of account management on a computer. Examples of account management events include:

A user account or group is created, changed, or deleted

A user account is renamed, disabled, or enabled

A password is set or changed

By default, this value is set to No auditing in the Default Domain Controller Group Policy object (GPO) and in the local policies of workstations and servers.

If you define this policy setting, you can specify whether to audit successes, audit failures, or not to audit the event type at all. Success audits generate an audit entry when any account management event is successful. Failure audits



generate an audit entry when any account management event fails. You can select No auditing by defining the policy setting and unchecking Success and Failure (Microsoft Developer's Network, 2000).

### ***Audit directory service access***

Determines whether to audit the event of a user accessing an Active Directory object that has its own system access control list (SACL) specified.

By default, this value is set to No auditing in the Default Domain Controller Group Policy object (GPO) and remains undefined for workstations and servers where it has no meaning.

If you define this policy setting, you can specify whether to audit successes, audit failures, or not to audit the event type at all. Success audits generate an audit entry when a user successfully accesses an Active Directory object that has a SACL specified. Failure audits generate an audit entry when a user unsuccessfully attempts to access an Active Directory object that has a SACL specified. You can select No auditing by defining the policy setting and unchecking Success and Failure.

Notes: You can set a SACL on an Active Directory object using the Security tab on the object's Properties page.

This is the same as Audit object access except it applies only to Active Directory objects rather than file system and registry objects (Microsoft Developer's Network, 2000).

### ***Audit logon events***

Determines whether to audit each instance of a user logging on, logging off, or making a network connection to this computer.

If you are auditing successful Audit account logon events on a domain controller, then workstation logons do not generate logon audits. Only interactive and network logons to the domain controller itself generate logon events. In short, "account logon events" are generated where the account lives. "Logon events" are generated where the logon occurs.

By default, this value is set to No auditing in the Default Domain Controller Group Policy object (GPO) and in the local policies of workstations and servers.

If you define this policy setting, you can specify whether to audit successes, audit failures, or not to audit the event type at all. Success audits generate an audit entry when logon occurs successfully. Failure audits generate an audit entry when an attempted occurrence of the logon fails. You can select No auditing by defining the policy setting and unchecking Success and Failure (Microsoft Developer's Network, 2000).

### ***Audit object access***

Determines whether to audit the event of a user accessing an object (for example, file, folder, registry key, printer, and so forth) which has its own system access control list (SACL) specified.

By default, this value is set to No auditing in the Default Domain Controller Group Policy object (GPO) and in the local policies of workstations and servers.

If you define this policy setting, you can specify whether to audit successes, audit failures, or not to audit the event type at all. Success audits generate an audit entry when a user successfully accesses an object that has a SACL specified. Failure audits generate an audit entry when a user unsuccessfully attempts to access an object that has a SACL specified. You can select No auditing by defining the policy setting and unchecking Success and Failure.

Note: You can set a SACL on a file system object using the Security tab on the object's Properties page (Microsoft Developer's Network, 2000).

### ***Audit policy change***

Determines whether to audit every incidence of a change to user rights assignment policies, audit policies, or trust policies.

By default, this value is set to No auditing in the Default Domain Controller Group Policy object (GPO) and in the local policies of workstations and servers.

If you define this policy setting, you can specify whether to audit successes, audit failures, or not to audit the event type at all. Success audits generate an audit entry when a change to user rights assignment policies, audit policies, or trust policies is successful. Failure audits generate an audit entry when a change to user rights assignment policies, audit policies, or trust policies fails. You can select No auditing by defining the policy setting and unchecking Success and Failure (Microsoft Developer's Network, 2000).

### ***Audit privilege use***

Determines whether to audit each instance of a user exercising a user right.

By default, this value is set to No auditing in the Default Domain Controller Group Policy object (GPO) and in the local policies of workstations and servers.

If you define this policy setting, you can specify whether to audit successes, audit failures, or not to audit the event type at all. Success audits generate an audit entry when a user right is successfully exercised. Failure audits generate an audit entry when the exercise of a user right fails. You can select No auditing by defining the policy setting and unchecking Success and Failure.

Note: By default, audits are not generated for use of the following user rights even if success or failure auditing is specified for audit privilege use:

- Bypass traverse checking
- Debug programs
- Create a token object
- Replace process level token
- Generate Security Audits
- Backup files and directories
- Restore files and directories

(Microsoft Developer's Network, 2000).

### ***Audit process tracking***

Determines whether to audit detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access.

By default, this value is set to No auditing in the Default Domain Controller Group Policy object

(GPO) and in the local policies of workstations and servers.

If you define this policy setting, you can specify whether to audit successes, audit failures, or not to audit the event type at all. Success audits generate an audit entry when the process being tracked is a success. Failure audits generate an audit entry when the process being tracked fails. You can select No auditing by defining the policy setting and unchecking Success and Failure (Microsoft Developer's Network, 2000).

#### ***Audit system events***

Determines whether to audit when a user restarts or shuts down the computer; or an event has occurred that affects either the system security or the security log.

By default, this value is set to No auditing in the Default Domain Controller Group Policy object (GPO) and in the local policies of workstations and servers.

If you define this policy setting, you can specify whether to audit successes, audit failures, or not to audit the event type at all. Success audits generate an audit entry when a system event is successfully executed. Failure audits generate an audit entry when a system event is unsuccessfully attempted. You can select No auditing by defining the policy setting and unchecking Success and Failure (Microsoft Developer's Network, 2000).

#### **(6) User Rights Assignment**

#### ***Access this computer from the network***

Determine which users and groups are allowed to connect to the computer over the network.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

The default groups that have this right on each platform are:

- Workstations and Servers
- Administrators
- Backup Operators

Power Users  
Users  
Everyone  
Domain Controllers  
Administrators  
Authenticated Users  
Everyone

(Microsoft Developer's Network, 2000).

***Act as part of the operating system***

This policy allows a process to authenticate as any user, and therefore gain access to the same resources as any user. Only low-level authentication services should require this privilege.

The potential access is not limited to what is associated with the user by default, because the calling process may request that arbitrary additional accesses be put in the access token. Of even more concern is that the calling process can build an anonymous token that can provide any and all accesses. Additionally, the anonymous token does not provide a primary identity for tracking events in the audit log.

Processes that require this privilege should use the LocalSystem account, which already includes this privilege, rather than using a separate user account with this privilege specially assigned.

By default, only the LocalSystem account has the privilege to act as part of the operating system (Microsoft Developer's Network, 2000).

***Add workstations to the domain***

Determines which groups or users can add workstations to a domain.

This policy is valid only on domain controllers. By default, any authenticated user has this right and can create up to ten computer accounts in the domain.

Adding a computer account to the domain allows the computer to participate in Active Directory based networking. For example, adding a workstation to a domain allows that workstation to recognize accounts and groups that exist in Active Directory.

The default group that has this right on domain controllers is:

Authenticated Users

Note: Users that have the "Create Computer Objects" permission on the Active Directory Computers container can also create computer accounts in the domain. The distinction is that users with permissions on the container are not restricted to the creation of only ten computer accounts. Furthermore, computer accounts created by means of the Add workstations to domain user right have Domain Administrators as the owner of the computer account, while computer accounts created by means of permissions on the computers container have the creator as the owner of the computer account. If a user has permissions on the container and also has the add workstation to domain user right, then the computer is added based on the computer container permissions rather than the user right (Microsoft Developer's Network, 2000).

### ***Backup files and directories***

Determines which users can circumvent file and directory permissions for the purposes of backing up the system.

Specifically, the privilege is similar to granting the following permissions to the user or group in question on all files and folders on the system:

- Traverse Folder/Execute File
- List Folder/Read Data
- Read Attributes
- Read Extended Attributes
- Read Permissions

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

The default groups that have this right on each platform are:

- Workstations and Servers
- Administrators
- Backup Operators
- Domain Controllers
- Administrators
- Backup Operators

(Microsoft Developer's Network, 2000).

### ***Bypass traverse checking***

Determines which users can traverse directory trees even though the user may not have permissions on the traversed directory. This privilege does not allow the user to list the contents of a directory, only to traverse directories.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

The default groups that have this right on each platform are:

- Workstations and Servers
- Administrators
- Backup Operators
- Power Users
- Users
- Everyone
- Domain Controllers
- Administrators
- Authenticated Users
- Everyone

(Microsoft Developer's Network, 2000).

### ***Change the system time***

Determines which users and groups can change the time and date on the internal clock of the computer.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

The default groups that have this right on each platform are:

- Workstations and Servers
- Administrators
- Power Users
- Domain Controllers
- Administrators
- Server Operators

(Microsoft Developer's Network, 2000).

### ***Create a pagefile***

Determines which users and groups can create and change the size of a pagefile. Creating a pagefile is accomplished by specifying a paging file size for a given drive in the **System Properties Performance Options**.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

The default is to allow administrators the ability to create a pagefile (Microsoft Developer's Network, 2000).

### ***Create a token object***

Determines which accounts can be used by processes to create a token which can then be used to get access to any local resources when the process uses NtCreateToken() or other token-creation APIs.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

It is recommended that processes requiring this privilege use the LocalSystem account, which already includes this privilege, rather than using a separate user account with this privilege specially assigned (Microsoft Developer's Network, 2000).

### ***Create permanent shared objects***

Determines which accounts can be used by processes to create a directory object in the Windows 2000 object manager.

This privilege is useful to kernel-mode components that plan to extend the Windows 2000 object name space. Because components running in kernel mode already have this privilege assigned to them, it is not necessary to specifically assign this privilege.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

By default, LocalSystem is the only account that has this right (Microsoft Developer's Network, 2000).

### ***Debug programs***

Determines which users can attach a debugger to any process. This privilege provides powerful access to sensitive and critical operating system components.



This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

By default, only administrators and LocalSystem accounts have the privileges to debug programs (Microsoft Developer's Network, 2000).

***Deny access to this computer from the network***

Determines which users are prevented from accessing a computer over the network. This policy setting supercedes the Access this computer from the network policy setting if a user account is subject to both policies.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers (Microsoft Developer's Network, 2000).

***Deny logon as a batch job***

Determines which accounts are prevented from being able to log on as a batch job. This policy setting supercedes the Log on as a batch job policy setting if a user account is subject to both policies.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

By default, there are no users denied logon as a batch job (Microsoft Developer's Network, 2000).

***Deny logon as a service***

Determines which service accounts are prevented from registering a process as a service. This policy setting supercedes the Log on as a service policy setting if an account is subject to both policies.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

By default, there are no accounts denied logon as a service (Microsoft Developer's Network, 2000).

***Deny logon locally***

Determines which users are prevented from logging on at the computer. This policy setting supercedes the Log on locally policy setting if an account is subject to both policies.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

By default, there are no accounts denied the ability to logon locally (Microsoft Developer's Network, 2000).

***Enable computer and user accounts to be trusted for delegation***

Determines which users can set the Trusted for Delegation setting on a user or computer object.

The user or object that is granted this privilege must have write access to the account control flags on the user or computer object. A server process running on a computer (or under a user context) that is trusted for delegation can access resources on another computer using a client's delegated credentials, as long as the client's account does not have the Account cannot be delegated account control flag set.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

The default groups that have this right on each platform are:

Workstations and Servers (none)

Domain Controllers (Administrators)

Note: Misuse of this privilege or of the Trusted for Delegation setting could make the network vulnerable to sophisticated attacks using Trojan horse programs that impersonate incoming clients and use their credentials to gain access to network resources (Microsoft Developer's Network, 2000).

***Force shutdown from a remote system***

Determines which users are allowed to shut down a computer from a remote location on the network.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

The default groups that have this right on each platform are:

Workstations and Servers (Administrators)

Domain Controllers (Administrators, Server Operators) (Microsoft Developer's Network, 2000).

### ***Generate security audits***

Determines which accounts can be used by a process to add entries to the security log. The security log is used to trace unauthorized system access.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

By default, only the LocalSystem account has the privilege to be used by processes to generate security audits (Microsoft Developer's Network, 2000).

### ***Increase quotas***

Determines which accounts can use a process with write property access to another process to increase the processor quota assigned to the other process.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

The default groups that have this right on each platform are:

Workstations and Servers (Administrators)

Domain Controllers (Administrators)

Note: This privilege is useful for system tuning, but can be abused as in a denial-of-service attack (Microsoft Developer's Network, 2000).

### ***Increase scheduling priority***

Determines which accounts can use a process with write property access to another process to increase the execution priority assigned to the other process. A user with this privilege can change the scheduling priority of a process through the Task Manager user interface.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

The default groups that have this right on each platform are:

Workstations and Servers (Administrators)

Domain Controllers (Administrators)

(Microsoft Developer's Network, 2000).

### ***Load and unload device drivers***

Determines which users can dynamically load and unload device drivers. This privilege is necessary for installing drivers for Plug and Play devices.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

The default groups that have this right on each platform are:

Workstations and Servers (Administrators)

Domain Controllers (Administrators)

(Microsoft Developer's Network, 2000).

### ***Lock pages in memory***

This privilege is obsolete and, therefore, is never checked.

This policy determines which accounts can use a process to keep data in physical memory, preventing the system from paging the data to virtual memory on disk. Exercising this privilege could significantly affect system performance (Microsoft Developer's Network, 2000).

### ***Log on as a batch job***

Allows a user to be logged on by means of a batch-queue facility.

For example, when a user submits a job by means of the task scheduler, the task scheduler logs that user on as a batch user rather than as an interactive user.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

By default, only the LocalSystem account has the privilege to be logged on as a batch job.

See also the Deny logon as a batch job policy.

Note: In the initial release of Windows 2000, the task scheduler automatically grants this right as necessary (Microsoft Developer's Network, 2000).

### ***Log on as a service***

Determines which service accounts can register a process as a service.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

By default, no accounts have the privilege to log on as a service (Microsoft Developer's Network, 2000).

### ***Log on locally***

Determine which users can log on at the computer.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

The default groups that have this right on each platform are:

#### Workstations and Servers

- Administrators
- Backup Operators
- Power Users
- Users
- Guest

#### Domain Controllers

- Account Operators
- Administrators
- Backup Operators
- Print Operators

Note: To allow a user to log on locally to a domain controller, you have to grant this right by means of the Default Domain Controller GPO (Microsoft Developer's Network, 2000).

### ***Manage audit and security log***

Determines which users can specify object access auditing options for individual resources such as files, Active Directory objects, and registry keys.

A user with this right can use the security tab in the security permission set editor's Properties dialog box to specify auditing options for the selected object.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

By default, only administrators have the privilege to manage auditing and the security log.

Note: This policy does not allow a user to specify that file and object access auditing be enabled in general. In order for such auditing to take place, the Audit object access setting under Audit Policies must be configured.

Audited events are viewed in the security log of the Event Viewer. A user with this policy can also view and clear the security log (Microsoft Developer's Network, 2000).

### ***Modify firmware environment values***

Allows a user to modify system-wide environment variables.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

By default, only administrators and LocalSystem accounts have the privilege to modify firmware environment variables (Microsoft Developer's Network, 2000).

### ***Profile single process***

Determines which users can use Windows NT and Windows 2000 performance monitoring tools to monitor the performance of non-system processes.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

By default, only administrators and LocalSystem accounts have the privilege to profile a single non-system process (Microsoft Developer's Network, 2000).

### ***Profile system performance***

Determines which users can use Windows NT and Windows 2000 performance monitoring tools to monitor the performance of system processes.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

By default, only administrators and LocalSystem accounts have the privilege to profile a single non-system process (Microsoft Developer's Network, 2000).

### ***Remove computer from docking station***

Determines which users can undock a laptop computer from its docking station.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

On servers and workstations, Administrators, Power Users, and Users have the right to remove a laptop computer from its docking station on computers that contain "clean installations" of Windows 2000 (that is, they weren't upgraded from a previous version of Windows). If you have upgraded the computer's operating system from Windows NT to Windows 2000, this right to remove the laptop computer from its docking station must be explicitly granted to the appropriate group or user (Microsoft Developer's Network, 2000).

### ***Replace a process level token***

Determines which user accounts can initiate a process to replace the default token associated with a launched sub-process.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

By default, only LocalSystem accounts have this privilege (Microsoft Developer's Network, 2000).

### ***Restore files and directories***

Determines which users can circumvent file and directory permissions when restoring backed up files and directories, and which users can set any valid security principal as the owner of an object.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

The default groups that have this right on each platform are:

Workstations and Servers (Administrators & Backup Operators)

Domain Controllers (Administrators, Backup Operators, Server Operators) (Microsoft Developer's Network, 2000).

### ***Shut down the system***

Determines which users logged on locally to the computer can shut down the operating system using the **Shut Down** command.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

The default groups that have this right on each platform are:

Workstations and Servers

Administrators

Backup Operators

Power Users

Users

Domain Controllers

Account Operators

Administrators

Backup Operators

Server Operators

Print Operators

(Microsoft Developer's Network, 2000).

### ***Synchronize Directory Service Data***

This policy setting is not used in the initial release of Windows 2000.

### ***Take ownership of files and other objects***

Determines which users can take ownership of any securable object in the system including



Active Directory objects, files and folders, printers, registry keys, processes, and threads.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

By default, only administrators have the privilege to take ownership of files or other objects (Microsoft Developer's Network, 2000).

(7) Security Options

***Additional restrictions for anonymous connections***

Determines what additional restrictions should be placed on anonymous connections to the computer. Windows 2000 allows anonymous users to perform certain activities such as enumerating the names of domain accounts and network shares. This is convenient, for example, when an administrator wants to grant access to users in a trusted domain that does not maintain a reciprocal trust. By default, an anonymous user has the same access that is granted to the Everyone group for a given resource. This security option allows additional restrictions to be placed on anonymous connections as follows: None. Rely on default permissions (Microsoft Developer's Network, 2000).

***Do not allow enumeration of SAM accounts and shares.***

This option replaces "Everyone" with "Authenticated Users" in the security permissions for resources. No access without explicit anonymous permissions. This option removes "Everyone" and "Network" from the anonymous users token; thus requiring that "Anonymous" be given explicit access to any required resources. This policy is defined by default in Local Computer Policy. By default, no additional restrictions are in place for anonymous connections (Microsoft Win2K Resource Kit, 2000).

***Allow server operators to schedule tasks (domain controllers only)***

Determines if Server Operators are allowed to submit jobs by means of the AT schedule facility.

By default, you must be an administrator in order to submit jobs by means of the AT scheduler. Enabling this security policy setting allows members of the Server Operators group to submit AT schedule jobs on Domain Controllers without having to make them Administrators. This policy is not defined by default (Microsoft Win2K Resource Kit, 2000).

***Allow system to shut down without having to log on***

Determines whether a computer can be shut down without having to log on to Windows. When this policy is enabled, the Shut Down command is available on the Windows logon screen. When this policy is disabled, the option to shut down the computer does not appear on the Windows logon screen. In this case, users must be able to log on to the computer successfully and have the Shut down the system user right in order to perform a system shutdown (Microsoft Win2K Resource Kit, 2000).

***Allowed to reject removable NTFS media***

Determines who is allowed to eject removable NTFS media from the computer. This policy is defined by default in Local Computer Policy. By default, only administrators have the right to eject removable NTFS media. This policy setting can be modified to provide any interactive user with the ability to eject removable NTFS media from the computer (Microsoft Win2K Resource Kit, 2000).

***Amount of idle time required before disconnecting session***

Determines the amount of continuous idle time that must pass in a Server Message Block (SMB) session before the session is disconnected due to inactivity. Administrators can use this policy to control when a computer disconnects an inactive SMB session. If client activity resumes, the session is automatically reestablished. This policy is defined for servers by default in Local Computer Policy with a default value of 15 minutes. This policy is not defined on workstations. For this policy setting, a value of 0 means to disconnect an

idle session as quickly as reasonably possible (Microsoft Win2K Resource Kit, 2000).

***Audit the access of global system objects***

Determines whether access of global system objects will be audited. When this policy is enabled, it causes system objects such as events, semaphores, and DOS Devices to be created with a default system access control list (SACL). If the Audit object access audit policy is also enabled, then access to these system objects will be audited. This policy is defined by default in Local Computer Policy where it is disabled by default (Microsoft Win2K Resource Kit, 2000).

***Audit use of backup and restore privilege***

Determines whether to audit every use of user rights including Backup and Restore. If you enable this policy, and if the Audit privilege use policy is enabled and in effect, then any instance of user rights being exercised will be recorded in the security log. If you disable this policy, when users use Backup or Restore privileges, those events will not be audited even when Audit Privilege Use is enabled. You should disable this policy if you want to contain the growth of the security log. This policy is defined by default in Local Computer Policy where it is disabled by default (Microsoft Win2K Resource Kit, 2000).

***Automatically log off users when log on time expires***

Determines whether to disconnect users that are connected to the local machine outside of their user account's valid logon hours. This setting affects the Server Message Block (SMB) component of a Windows 2000 server. When this policy is enabled, it causes client sessions with the SMB server to be forcibly disconnected when the client's logon hours expire. If this policy is disabled, an established client session is allowed to be maintained after the client's logon hours have expired (Microsoft Win2K Resource Kit, 2000).

***Automatically log off users when log on time expires (local)***

Determines whether to disconnect users that are connected to the local machine outside of their user account's valid logon hours. This setting affects the Server Message Block (SMB) component of a Windows 2000 server. When this policy is enabled, it causes client sessions with the SMB server to be forcibly disconnected when the client's logon hours expire. If this policy is disabled, an established client session is allowed to be maintained after the client's logon hours have expired. This policy is defined by default in Local Computer Policy, where it is enabled by default (Microsoft Win2K Resource Kit, 2000).

***Clear virtual memory pagefile when system shuts down***

Determines whether the virtual memory pagefile should be cleared when the system is shut down. Windows 2000 virtual memory support uses a system pagefile to swap pages of memory to disk when they are not being actively used. On a running system, this pagefile is opened exclusively by the operating system and is well protected. However, systems that are configured to allow booting to other operating systems might want to ensure that system pagefile is wiped clean when Windows 2000 shuts down. This ensures that sensitive information from process memory that might have made it into the pagefile is not available to an unauthorized user who has managed to directly access the page file. When this policy is enabled, it causes the system pagefile to be cleared upon clean shutdown. Enabling this security option also causes the hibernation file (hiberfil.sys) to be zeroed out when hibernation is disabled on a laptop system. When this policy is disabled, the virtual memory pagefile is not cleared during system shutdown. This policy is defined by default in Local Computer Policy, where it is disabled by default (Microsoft Win2K Resource Kit, 2000).

***Digitally sign client communications (always)***

If this policy is enabled, it requires the Windows 2000 Server Message Block (SMB) server to perform SMB packet signing. This policy is defined by default in Local Computer Policy,

where it is disabled by default (Microsoft Win2K Resource Kit, 2000).

***Digitally sign client communications  
(when possible)***

If this policy is enabled, it causes the Windows 2000 Server Message Block (SMB) server to perform SMB packet signing. This policy is disabled by default on workstation and server platforms in Local Computer Policy. This policy is enabled by default on Domain Controllers in the Default Domain Controllers Group Policy object (GPO) (Microsoft Win2K Resource Kit, 2000).

***Digitally sign server communications  
(always)***

Determines whether the computer will always digitally sign client communications. The Windows 2000 Server Message Block (SMB) authentication protocol supports mutual authentication, which closes a "man-in-the-middle" attack, and supports message authentication, which prevents active message attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. In order to use SMB signing, you must either enable it or require it on both the SMB client and the SMB server. If SMB signing is enabled on a server, then clients that are also enabled for SMB signing will use the packet signing protocol during all subsequent sessions. If SMB signing is required on a server, then a client will not be able to establish a session unless it is at least enabled for SMB signing. If this policy is enabled, it requires the Windows 2000 SMB client to perform SMB packet signing. If this policy is disabled, it does not require the SMB client to sign packets. This policy is defined by default in Local Computer Policy, where it is disabled by default (Microsoft Win2K Resource Kit, 2000).

***Digitally sign server communications  
(when possible)***

If this policy is enabled, it causes the Windows 2000 Server Message Block (SMB) client to perform SMB packet signing when communicating with an SMB server that is enabled

or required to perform SMB packet signing. This policy is defined by default in Local Computer Policy, where it is enabled by default (Microsoft Win2K Resource Kit, 2000).

***Disable CTRL+ALT+DEL requirement for logon***

Determines whether pressing CTRL+ALT+DEL is required before a user can log on. If this policy is enabled on a computer, a user is not required to press CTRL+ALT+DEL in order to log on. Not having to press CTRL+ALT+DEL leaves the user susceptible to attacks that attempt to intercept the user's password. Requiring CTRL+ALT+DEL before logon ensures that the user is communicating by means of a trusted path when entering their password. If this policy is disabled, then any user is required to press CTRL+ALT+DEL before logging on to Windows (unless they are using a smart card for Windows logon). This policy is disabled by default on workstations and servers that are joined to a domain. It is enabled by default on stand-alone workstations (Microsoft Win2K Resource Kit, 2000).

***Do not display last user name in logon screen***

Determines whether the name of the last user to logon to the computer is displayed in the Windows logon screen. If this policy is enabled, the name of the last user to successfully logon is not displayed in the Log On to Windows dialog box. If this policy is disabled, the name of the last user to logon is displayed. This policy is defined by default in Local Computer Policy, where it is disabled by default (Microsoft Win2K Resource Kit, 2000).

***LAN Manager Authentication level***

Determines which challenge/response authentication protocol is used for network logons. The choice affects the level of authentication protocol used by clients, the level of session security negotiated, and the level of authentication accepted by servers as follows:

Send LM & NTLM responses: Clients use LM and NTLM authentication, and never use NTLMv2 session security; Domain Controllers

(DCs) accept LM, NTLM, and NTLMv2 authentication.

Send LM & NTLM - use NTLMv2 session security if negotiated: Clients use LM and NTLM authentication, and use NTLMv2 session security if server supports it; DCs accept LM, NTLM, and NTLMv2 authentication.

Send NTLM response only: Clients use NTLM authentication only, and use NTLMv2 session security if server supports it; DCs accept LM, NTLM, and NTLMv2 authentication.

Send NTLMv2 response only: Clients use NTLMv2 authentication only, and use NTLMv2 session security if server supports it; DCs accept LM, NTLM, and NTLMv2 authentication.

Send NTLMv2 response only\refuse LM: Clients use NTLMv2 authentication only, and use NTLMv2 session security if server supports it; DCs refuse LM (accept only NTLM and NTLMv2 authentication).

Send NTLMv2 response only\refuse LM & NTLM: Clients use NTLMv2 authentication only, and use NTLMv2 session security if server supports it; DCs refuse LM and NTLM (accept only NTLMv2 authentication).

The default setting for servers is Send LM & NTLM responses. This setting can affect the ability of Windows 2000 computers to communicate with Windows NT 4.0 and earlier clients over the network. For example, at the time of this writing, Windows NT 4.0 computers prior to SP4 do not support NTLMv2. Win9x computers do not support NTLM (Microsoft Win2K Resource Kit, 2000).

### ***Message text for users attempting to logon***

Specifies a text message that is displayed to users when they log on. This text is often used for legal reasons, such as to warn users about the ramifications of misusing company information or to warn them that their actions may be audited. For servers, this policy is enabled but there is no default text specified. This policy is not defined for workstations by default (Microsoft Win2K Resource Kit, 2000).

***Message title for users attempting to logon***

Allows the specification of a title to appear in the title bar of the window that contains the Message text for users attempting to log on. For servers, this policy is enabled but there is no default text specified. This policy is not defined for workstations by default (Microsoft Win2K Resource Kit, 2000).

***Number of previous logons to cache (in case domain controller is not available)***

Determines the number of times a user can log on to a Windows domain using cached account information. Windows 2000 caches previous users' logon information locally so that they will be able to log on in the event that a domain controller is unavailable during subsequent logon attempts. If a domain controller is unavailable and a user's logon information is cached, the user will be prompted with a dialog that reads: A domain controller for your domain could not be contacted. You have been logged on using cached account information. Changes to your profile since you last logged on may not be available. If a domain controller is unavailable and a user's logon information is not cached, the user is prompted with this message: The system cannot log you on now because the domain <DOMAIN\_NAME> is not available.

In this policy setting, a value of 0 disables logon caching. Any value above 50 will only cache 50 logon attempts. For servers, this policy is defined by default in Local Computer Policy and the default value is 10 logons (Microsoft Win2K Resource Kit, 2000).

***Prevent system maintenance of computer account password***

Determines whether the computer account password should be prevented from being reset every week. As a part of Windows 2000 security, computer account passwords are changed automatically every seven days. If this policy is enabled, the machine is prevented from requesting a weekly password change. If this policy is disabled, a new password for the computer account will be



generated every week. This policy is defined by default in Local Computer Policy where it is disabled by default (Microsoft Win2K Resource Kit, 2000).

***Prevent users from installing print drivers***

Determines whether members of the Users group are prevented from installing print drivers. If this policy is enabled, it prevents users from installing printer drivers on the local machine. This prevents users from "Adding Printers" when the device driver does not exist on the local machine. If this policy is disabled, then a member of the Users group can install printer drivers on the computer. By default, this setting is enabled on servers and disabled on workstations (Microsoft Win2K Resource Kit, 2000).

***Prompt user to change password before expiration***

Determines how far in advance Windows 2000 should warn users that their password is about to expire. By giving the user advanced warning, the user has time to construct a sufficiently strong password. By default, this value is set to 14 days (Microsoft Win2K Resource Kit, 2000).

***Recovery console: Allow automatic administrative logon***

By default, the Recovery Console requires you to provide the password for the Administrator account before accessing the system. If this option is set, the Recovery Console does not require you to provide a password and will automatically log on to the system (Microsoft Win2K Resource Kit, 2000).

***Recovery console: Allow floppy copy and access to all drivers and all folders***

Enabling this option enables the Recovery Console SET command, which allows you to set the following Recovery Console environment variables:

AllowWildCards - Enable wildcard support for some commands (such as the DEL command).

AllowAllPaths - Allow access to all files and folders on the computer.

AllowRemovableMedia - Allow files to be copied to removable media, such as a floppy disk.

NoCopyPrompt - Do not prompt when overwriting an existing file.

By default, the SET command is disabled and all these variables are not enabled(Microsoft Win2K Resource Kit, 2000).

Rename administrators account

Determines whether a different account name will be associated with the security identifier (SID) for the account "Administrator." By associating the Administrator SID with another account, you will no longer have an account named "Administrator," which is often a point of attack by hackers (Microsoft Win2K Resource Kit, 2000).

***Rename administrator account***

Determines whether a different account name will be associated with the security identifier (SID) for the account "Administrator." By associating the Administrator SID with another account, you will no longer have an account named "Administrator," which is often a point of attack by hackers (Microsoft Win2K Resource Kit, 2000).

***Rename guest account***

Determines whether a different account name will be associated with the security identifier (SID) for the account "Guest." By associating the Guest SID with another account, you will no longer have an account named "Guest," which is often a point of attack by hackers (Microsoft Win2K Resource Kit, 2000).

***Restrict CD-Rom access to locally logged on user only***

Determines whether a CD-ROM is accessible to both local and remote users simultaneously. If enabled, this policy allows only the interactively logged-on user to access removable CD-ROM media. If no one is logged on interactively, the CD-ROM may be shared over the network. If this policy is disabled, then the local user and remote users can access the CD-ROM simultaneously (Microsoft Win2K Resource Kit, 2000).

***Restrict floppy access to locally logged on user only***

Determines whether removable floppy media is accessible to both local and remote users simultaneously. If enabled, this policy allows only the interactively logged-on user to access removable floppy media. If no one is logged on interactively, the floppy media may be shared over the network. If this policy is disabled, then the local user and remote users can access the floppy media simultaneously (Microsoft Win2K Resource Kit, 2000).

***Secure channel: Digitally encrypt or sign secure channel data (always)***

Determines whether the computer will always digitally encrypt or sign secure channel data. When a Windows 2000 system joins a domain, a computer account is created. Thereafter, when the system boots, it uses the password for that account to create a secure channel with the domain controller for its domain. Requests sent on the secure channel are authenticated, and sensitive information (such as passwords) is encrypted, but the channel is not integrity checked and not all information is encrypted. If this policy is enabled, all outgoing secure channel traffic must be either signed or encrypted. If this policy is disabled, signing and encryption are negotiated with the domain controller. By default, this policy is disabled. This option should only be enabled if all of the domain controllers in all the trusted domains support signing and sealing. If this parameter is enabled, then Secure channel: Digitally sign secure channel data (when possible) is automatically enabled (Microsoft Win2K Resource Kit, 2000).

***Secure channel: Digitally encrypt secure channel data (when possible)***

Determines whether the computer will always digitally encrypt or sign secure channel data. When a Windows 2000 system joins a domain, a computer account is created. Thereafter, when the system boots, it uses the password for that account to create a secure channel with the domain controller for its domain. Requests sent on the secure channel are authenticated, and sensitive information (such as passwords) is encrypted, but the channel is not integrity checked and not all

information is encrypted. If this policy is enabled, all outgoing secure channel traffic should be encrypted. If this policy is disabled, outgoing secure channel traffic will not be encrypted. By default, this option is enabled (Microsoft Win2K Resource Kit, 2000).

***Secure channel: Digitally sign secure channel data (when possible)***

Determines whether the computer will always digitally encrypt or sign secure channel data. When a Windows 2000 system joins a domain, a computer account is created. Thereafter, when the system boots, it uses the password for that account to create a secure channel with the domain controller for its domain. Requests sent on the secure channel are authenticated, and sensitive information (such as passwords) is encrypted, but the channel is not integrity checked and not all information is encrypted. If this policy is enabled, all outgoing secure channel traffic should be signed. If this policy is disabled, no outgoing secure channel traffic will be signed. By default, this option is enabled. If Secure channel: Digitally encrypt secure channel data (when possible) is enabled, it will override any setting for this option and force it to be enabled (Microsoft Win2K Resource Kit, 2000).

***Secure channel: Require strong (Windows 2000 or later) session key***

If this policy is enabled, all outgoing secure channel traffic will require a strong (Windows 2000 or later) encryption key. If this policy is disabled, the key strength is negotiated with the DC. This option should only be enabled if all of the DCs in all trusted domains support strong keys. By default, this value is disabled (Microsoft Win2K Resource Kit, 2000).

***Secure system partition (for RISC Platforms only)***

If this policy is enabled, only administrative access is allowed to a RISC-based system partition (which must be FAT) while the operating system is running (Microsoft Win2K Resource Kit, 2000).

***Send unencrypted password to connect to third party SMB servers***

If this policy is enabled, the Server Message Block (SMB) redirector is allowed to send clear-text passwords to non-Microsoft SMB servers which do not support password encryption during authentication. By default, this option is disabled (Microsoft Win2K Resource Kit, 2000).

***Shut down system immediately if unable to log security audits***

Determines whether the system should shut down if it is unable to log security events. If this policy is enabled, it causes the system to halt if a security audit cannot be logged for any reason. Typically, an event will fail to be logged when the security audit log is full and the retention method specified for the security log is either Do Not Overwrite Events or Overwrite Events by Days. If the security log is full and an existing entry cannot be overwritten and this security option is enabled, the following blue screen error will occur:

STOP: C0000244 {Audit Failed}  
An attempt to generate a security audit failed.

To recover, an administrator must log on, archive the log (if desired), clear the log, and reset this option as desired. By default, this policy is disabled (Microsoft Win2K Resource Kit, 2000).

***Smart card removal behavior***

Determines what should happen when the smart card for a logged-on user is removed from the smart card reader. The options are: 1) No Action 2) Lock Workstation 3) Force Logoff 4) By default, No Action is specified. If Lock Workstation is specified, then the workstation is locked when the smart card is removed allowing users to leave the area, take their smart card with them, and still maintain a protected session. If Force Logoff is specified, then the user is automatically logged off when the smart card is removed (Microsoft Win2K Resource Kit, 2000).

***Strengthen default permissions of global system objects (e.g. Symbolic links)***

Determines the strength of the default discretionary access control list (DACL) for objects.

Windows 2000 maintains a global list of shared system resources such as DOS device names, mutexes, and semaphores. In this way, objects can be located and shared among processes. Each type of object is created with a default DACL that specifies who can access the objects with what permissions. If this policy is enabled, the default DACL is stronger, allowing non-admin users to read shared objects, but not modify shared objects that they did not create. By default, this option is enabled (Microsoft Win2K Resource Kit, 2000).

***Unsigned driver installation behavior***

Determines what should happen when an attempt is made to install a device driver (by means of the Windows 2000 device installer) that has not been certified by the Windows Hardware Quality Lab (WHQL). The options are: 1) Silently succeed 2) Warn but allow installation 3) Do not allow installation 4) The default setting is to Warn but allow installation (Microsoft Win2K Resource Kit, 2000).

***Unsigned non-driver installation behavior***

Determines what should happen when an attempt is made to install any non-device driver software that has not been certified. The options are: 1) Silently succeed 2) Warn but allow installation 3) Do not allow installation 4) The default setting is to Silently succeed (Microsoft Win2K Resource Kit, 2000).

***Event Logs***  
(8)

Settings for Event Logs

***Maximum application log size***

Specifies the maximum size for the application event log. The default is 512KB, and the maximum size is 4GB.

Note: The Event Log folder that contains this policy is available only in Group Policy objects associated with domains, OUs, and sites. The Event Log folder does not appear in the Local Computer Policy object (Microsoft Developer's Network, 2000).

***Maximum security log size***

Specifies the maximum size for the security event log. The default is 512KB, and the maximum size is 4GB.

Note: The Event Log folder that contains this policy is available only in Group Policy objects associated with domains, OUs, and sites. The Event Log folder does not appear in the Local Computer Policy object (Microsoft Developer's Network, 2000).

### ***Maximum system log size***

Specifies the maximum size for the system event log. The default is 512KB, and the maximum size is 4GB.

Note: The Event Log folder that contains this policy is available only in Group Policy objects associated with domains, OUs, and sites. The Event Log folder does not appear in the Local Computer Policy object (Microsoft Developer's Network, 2000).

### ***Restrict guest access to application log***

If this policy is enabled, guests are prevented from access to the application event log.

By default, this policy is disabled.

Note: The Event Log folder that contains this policy is available only in Group Policy objects associated with domains, OUs, and sites. The Event Log folder does not appear in the Local Computer Policy object (Microsoft Developer's Network, 2000).

### ***Restrict guest access to security log***

If this policy is enabled, guests are prevented from access to the security event log.

By default, this policy is disabled.

Note: A user must possess the Manage auditing and security log user right in order to access the security log. The Event Log folder that contains this policy is available only in Group Policy objects associated with domains, OUs, and sites. The Event Log folder does not appear in the Local Computer Policy object (Microsoft Developer's Network, 2000).

### ***Restrict guest access to system log***

If this policy is enabled, guests are prevented from access to the system event log.

By default, this policy is disabled.

Note: The Event Log folder that contains this policy is available only in Group Policy objects associated with domains, OUs, and sites. The Event Log folder does not appear in the Local Computer Policy object (Microsoft Developer's Network, 2000).

### ***Retain application log***

Determines the number of days' worth of events that should be retained for the application log if the retention method for the application log is "By Days."

Set this value only if you archive the log at scheduled intervals and make sure that the Maximum application log size is large enough to accommodate the interval.

Note: The Event Log folder that contains this policy is available only in Group Policy objects associated with domains, OUs, and sites. The Event Log folder does not appear in the Local Computer Policy object (Microsoft Developer's Network, 2000).

### ***Retain system log***

Determines the number of days' worth of events that should be retained for the security log if the retention method for the security log is "By Days."

Set this value only if you archive the log at scheduled intervals and make sure that the maximum security log size is large enough to accommodate the interval.

Note: The Event Log folder that contains this policy is available only in Group Policy objects associated with domains, OUs, and sites. The Event Log folder does not appear in the Local Computer Policy object (Microsoft Developer's Network, 2000).

### ***Retain security log***

Determines the number of days' worth of events that should be retained for the system log if the retention method for the system log is "By Days."

Set this value only if you archive the log at scheduled intervals and make sure that the



Maximum system log size is large enough to accommodate the interval.

Note: The Event Log folder that contains this policy is available only in Group Policy objects associated with domains, OUs, and sites. The Event Log folder does not appear in the Local Computer Policy object (Microsoft Developer's Network, 2000).

### ***Retention method for application log***

Determines the "wrapping" method for the application log.

If you do not archive the application log, specify Overwrite events as needed.

If you archive the log at scheduled intervals, specify Overwrite events by days and specify the appropriate number of days in the retain application log setting. Make sure the Maximum application log size is large enough to accommodate the interval.

If you must retain all the events in the log, select Do not overwrite events. This option requires that the log be cleared manually. In this case, when the maximum log size is reached, new events will be discarded.

Note: The Event Log folder that contains this policy is available only in Group Policy objects associated with domains, OUs, and sites. The Event Log folder does not appear in the Local Computer Policy object (Microsoft Developer's Network, 2000).

### ***Retention method for security log***

Determines the "wrapping" method for the security log.

If you do not archive the security log, specify Overwrite events as needed.

If you archive the log at scheduled intervals, specify Overwrite events by days and specify the appropriate number of days in the retain security log setting. Make sure the Maximum security log size is large enough to accommodate the interval.

If you must retain all the events in the log, select Do not overwrite events. This option requires that the log be cleared manually. In this case, when the maximum log size is reached, new events will be discarded.

Note: The Event Log folder that contains this policy is available only in Group Policy objects associated with domains, OUs, and sites. The Event Log folder does not appear in the Local Computer Policy object (Microsoft Developer's Network, 2000).

### ***Retention method for system log***

Determines the "wrapping" method for the system log.

If you do not archive the system log, specify Overwrite events as needed.

If you archive the log at scheduled intervals, specify Overwrite events by days and specify the appropriate number of days in the retain system log setting. Make sure the Maximum system log size is large enough to accommodate the interval.

If you must retain all the events in the log, select Do not overwrite events. This option requires that the log be cleared manually. In this case, when the maximum log size is reached, new events will be discarded.

Note: The Event Log folder that contains this policy is available only in Group Policy objects associated with domains, OUs, and sites. The Event Log folder does not appear in the Local Computer Policy object (Microsoft Developer's Network, 2000).

### ***Shut down the computer when the security audit log is full***

Use Shut down system immediately if unable to log security audits instead of this policy setting.

Note: The Event Log folder that contains this policy is available only in Group Policy objects associated with domains, OUs, and sites. The Event Log folder does not appear in the Local Computer Policy object (Microsoft Developer's Network, 2000).

*Restricted Groups*  
*System Services*  
*Registry*  
*File System*  
*Public Key Policies*  
*IP Security Policies on Active Directory*

## **ADMINISTRATIVE TEMPLATES**

### **Windows Components**

#### *Net Meeting*

##### ***Disable remote desktop sharing***

Disables the remote desktop sharing feature of NetMeeting. Users will not be able to set it up or use it for controlling their computers remotely. The NetMeeting folder containing this policy is created by the Conf.adm administrative template. Conf.adm is included in Windows 2000, but does not load in Group Policy automatically. To display the NetMeeting folder, add the Conf.adm administrative template to Group Policy (Microsoft Developer's Network, 2000).

#### *Internet Explorer*

##### ***Security Zones: Use only machine settings***

Applies security zone information to all users of the same computer. A security zone is a group of Web sites with the same security level.

If you enable this policy, changes that the user makes to a security zone will apply to all users of that computer.

If you disable this policy or do not configure it, users of the same computer can establish their own security zone settings.

This policy is intended to ensure that security zone settings apply uniformly to the same computer and do not vary from user to user (Microsoft Developer's Network, 2000).

##### ***Security Zones: Do not allow users to change policies***

Prevents users from changing security zone settings. A security zone is a group of Web sites with the same security level.

If you enable this policy, the Custom Level button and security-level slider on the Security tab in the Internet Options dialog box are disabled.

If you disable this policy or do not configure it, users can change the settings for security zones.

This policy prevents users from changing security zone settings established by the administrator.

Note: The "Disable the Security page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Security tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored (Microsoft Developer's Network, 2000).

### ***Security Zones: Do not allow users to add/delete sites***

Prevents users from adding or removing sites from security zones. A security zone is a group of Web sites with the same security level.

If you enable this policy, the site management settings for security zones are disabled. (To see the site management settings for security zones, in the Internet Options dialog box, click the Security tab, and then click the Sites button.)

If you disable this policy or do not configure it, users can add Web sites to or remove sites from the Trusted Sites and Restricted Sites zones, and alter settings for the Local Intranet zone.

This policy prevents users from changing site management settings for security zones established by the administrator.

Note: The "Disable the Security page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Security tab from the interface, takes precedence over this policy. If it is enabled, this policy is ignored (Microsoft Developer's Network, 2000).

### ***Make proxy settings per machine***

Applies proxy settings to all users of the same computer.

If you enable this policy, users cannot set user-specific proxy settings. They must use the zones created for all users of the computer.

If you disable this policy or do not configure it, users of the same computer can establish their own proxy settings.

This policy is intended to ensure that proxy settings apply uniformly to the same computer and do not vary from user to user (Microsoft Developer's Network, 2000).

### ***Disable automatic install of Internet Explorer components***

Prevents Internet Explorer from automatically installing components.

If you enable this policy, it prevents Internet Explorer from downloading a component when users browse to a Web site that needs that component.

If you disable this policy or do not configure it, users will be prompted to download and install a component when visiting a Web site that uses that component.

This policy is intended to help the administrator control which components the user installs (Microsoft Developer's Network, 2000).

### ***Disable periodic check for IE software updates***

Prevents Internet Explorer from checking whether a new version of the browser is available.

If you enable this policy, it prevents Internet Explorer from checking to see whether it is the latest available browser version and notifying users if a new version is available.

If you disable this policy or do not configure it, Internet Explorer checks every 30 days by default, and then notifies users if a new version is available.

This policy is intended to help the administrator maintain version control for Internet Explorer by preventing users from being notified about new versions of the browser (Microsoft Developer's Network, 2000).

### ***Disable software update shell notifications on program launch***

Specifies that programs using the Microsoft Software Distribution Channel will not notify users when they install new components. The Software Distribution Channel is a means of updating software dynamically on users' computers by using Open Software Distribution (.osd) technologies.

If you enable this policy, users will not be notified if their programs are updated using Software Distribution Channels.

If you disable this policy or do not configure it, users will be notified before their programs are updated.

This policy is intended for administrators who want to use Software Distribution Channels to update their users'

programs without user intervention (Microsoft Developer's Network, 2000).

### ***Disable showing the splash screen***

Prevents the Internet Explorer splash screen from appearing when users start the browser.

If you enable this policy, the splash screen, which displays the program name, licensing, and copyright information, is not displayed.

If you disable this policy or do not configure it, the splash screen will be displayed when users start their browsers (Microsoft Developer's Network, 2000).

## ***Task Scheduler***

### ***Hide property pages***

Prevents users from viewing and changing the properties of an existing task.

This policy removes the Properties item from the File menu in Scheduled Tasks and from the context menu that appears when you right-click a task. As a result, users cannot change any properties of a task. They can only see the properties that appear in Detail view and in the task preview.

This policy prevents users from viewing and changing characteristics such as the program the task runs, its schedule details, idle time and power management settings, and its security context.

Note: This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Tip: This policy affects existing tasks only. To prevent users from changing the properties of newly created tasks, use the "Disable Advanced Menu" policy (Microsoft Developer's Network, 2000).

### ***Prevent task run or end***

Prevents users from starting and stopping tasks manually.

This policy removes the Run and End Task items from the context menu that appears when you right-click a task. As a result, users cannot start tasks manually or force tasks to end before they are finished.

Note: This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer

Configuration takes precedence over the setting in User Configuration (Microsoft Developer's Network, 2000).

### ***Disable drag and drop***

Prevents users from adding or removing tasks by moving or copying programs in the Scheduled Tasks folder.

This policy disables the Cut, Copy, Paste, and Paste shortcut items on the context menu and the Edit menu in Scheduled Tasks. It also disables the drag-and-drop features of the Scheduled Tasks folder.

As a results, users cannot add new scheduled tasks by dragging, moving, or copying a document or program into the Scheduled tasks folder.

This policy does not prevent users from using other methods to create new tasks and it does not prevent users from deleting tasks.

Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration (Microsoft Developer's Network, 2000).

### ***Disable new task creation***

Prevents users from creating new tasks.

This policy removes the Add Scheduled Task item that starts the New Task wizard. Also, the system does not respond when users try to move, paste, or drag programs or documents into the Scheduled Tasks folder.

Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Important: This policy does not prevent administrators of a computer from using At.exe to create new tasks or prevent administrators from submitting tasks from remote computers (Microsoft Developer's Network, 2000).

### ***Disable task deletion***

Prevents users from deleting tasks from the Scheduled Tasks folder.

This policy removes the Delete item from the Edit menu in the Scheduled Tasks folder and from the menu that appears when you right-click a task. Also, the system does not respond when users try to cut or drag a task from the Scheduled Tasks folder.

Note: This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Important: This policy does not prevent administrators of a computer from using At.exe to delete tasks (Microsoft Developer's Network, 2000).

### ***Disable advanced menu***

Prevents users from viewing or changing the properties of newly created tasks.

This policy removes the "Open advanced properties for this task when I click Finish" item from the last page of the Scheduled Task wizard.

This policy prevents users from viewing and changing task characteristics, such as the program the task runs, details of its schedule, idle time and power management settings, and its security context. It is designed to simplify task creation for beginning users.

Note: This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Tip: This policy affects newly created tasks only. To prevent users from changing the properties of existing tasks, use the "Hide Property Pages" policy (Microsoft Developer's Network, 2000).

### ***Prohibit browse***

Limits newly scheduled items on the user's Start menu and prevents the user from changing the scheduled program for existing tasks.

This policy removes the Browse button from the Schedule Task wizard and from the Task tab of the properties dialog box for a task. Also, users cannot edit the "Run" box or the "Start in" box that determine the program and path for a task.

As a result, when users create a task, they must select a program from the list in the Scheduled Task wizard, which displays only the tasks that appear on the Start menu and its submenus. Once a task is created, users cannot change the program a task runs.

Important: This policy does not prevent users from creating a new task by pasting or dragging any program



into the Scheduled Tasks folder. To prevent this action, use the "Disable Drag-and-Drop" policy.

Note: This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration (Microsoft Developer's Network, 2000).

### ***Windows Installer***

#### ***Disable windows installer***

Disables or restricts the use of Windows Installer.

This policy can prevent users from installing software on their systems or permit users to install only those programs offered by a system administrator.

If you enable this policy, you can use the options in the Disable Windows Installer box to establish an installation policy.

- The "Never" option indicates that Windows Installer is fully enabled. Users can install and upgrade software. Windows Installer is enabled by default on Windows 2000.

- The "For non-managed apps only" option permits users to install only those programs that a system administrator assigns (offers on the desktop) or publishes (adds them to Add/Remove Programs).

- The "Always" option indicates that Windows Installer is disabled.

This policy affects Windows Installer only. It does not prevent users from using other methods to install and upgrade programs (Microsoft Developer's Network, 2000).

#### ***Always install with elevated privileges***

Directs Windows Installer to use system permissions when it installs any program on the system.

This policy extends elevated privileges to all programs. These privileges are usually reserved for programs that have been assigned to the user (offered on the desktop), assigned to the computer (installed automatically), or made available in Add/Remove Programs in Control Panel. This policy lets users install programs that require access to directories that the user might not have permission to view or change, including directories on highly restricted computers.

If you disable this policy or do not configure it, the system applies the current user's permissions when it installs programs that a system administrator does not distribute or offer.

Note: This policy appears both in the Computer Configuration and User Configuration folders. To make this policy effective, you must enable the policy in both folders.

Caution: Skilled users can take advantage of the permissions this policy grants to change their privileges and gain permanent access to restricted files and folders. Note that the User Configuration version of this policy is not guaranteed to be secure (Microsoft Developer's Network, 2000).

### ***Disable rollback***

Prohibits Windows Installer from generating and saving the files it needs to reverse an interrupted or unsuccessful installation.

This policy prevents Windows Installer from recording the original state of the system and sequence of changes it makes during installation. It also prevents Windows Installer from retaining files it intends to delete later. As a result, Windows installer cannot restore the computer to its original state if the installation does not complete.

This policy is designed to reduce the amount of temporary disk space required to install programs. Also, it prevents malicious users from interrupting an installation to gather data about the internal state of the computer or to search secure system files. However, because an incomplete installation can render the system or a program inoperable, do not use this policy unless essential.

This policy appears in the Computer Configuration and User Configuration folders. If the policy is enabled in either folder, it is considered be enabled, even if it is explicitly disabled in the other folder (Microsoft Developer's Network, 2000).

### ***Disable browse dialog box for new source***

Prevents users from searching for installation files when they add features or components to an installed program.

This policy disables the Browse button beside the Use feature from list in the Windows Installer dialog box. As a result, users must select an installation file source from the Use features from list that the system administrator configures.

This policy applies even when the installation is running in the user's security context.

If you disable this policy or do not configure it, the Browse button is enabled when an installation is running in the user's security context, but only system administrators can browse when an installation is running with elevated system privileges, such as installations offered on the desktop or in Add/Remove Programs.

This policy affects Windows Installer only. It does not prevent users from selecting other browsers, such as Windows Explorer or My Network Places, to search for installation files (Microsoft Developer's Network, 2000).

### ***Disable patching***

Prevents users from using Windows Installer to install patches.

Patches are updates or upgrades that replace only those program files that have changed. Because patches can be easy vehicles for malicious programs, some installations prohibit their use.

Note: This policy applies only to installations that run in the user's security context. By default, users who are not system administrators cannot apply patches to installations that run with elevated system privileges, such as those offered on the desktop or in Add/Remove Programs (Microsoft Developer's Network, 2000).

### ***Disable IE security prompt for windows installer script***

Allows Web-based programs to install software on the computer without notifying the user.

By default, when a script hosted by an Internet browser tries to install a program on the system, the system warns users and allows them to select or refuse the installation. This policy suppresses the warning and allows the installation to proceed.

This policy is designed for enterprises that use Web-based tools to distribute programs to their employees. However, because this policy can pose a security risk, it should be applied cautiously (Microsoft Developer's Network, 2000).

### ***Enable user control over installs***

Permits users to change installation options that typically are available only to system administrators.

This policy bypasses some of the security features of Windows Installer. It permits installations to complete that otherwise would be halted due to a security violation.

The security features of Windows Installer prevent users from changing installation options typically reserved

for system administrators, such as specifying the directory to which files are installed. If Windows Installer detects that an installation package has permitted the user to change a protected option, it stops the installation and displays a message. These security features operate only when the installation program is running in a privileged security context in which it has access to directories denied to the user.

This policy is designed for less restrictive environments. It can be used to circumvent errors in an installation program that prevent software from being installed (Microsoft Developer's Network, 2000).

***Enable user to browse the source while elevated***

Allows users to search for installation files during privileged installations.

This policy enables the Browse button on the "Use feature from" dialog box. As a result, users can search for installation files, even when the installation program is running with elevated system privileges. By default, only system administrators can browse during installations with elevated privileges, such as installations offered on the desktop or displayed in Add/Remove Programs.

Because the installation is running with elevated system privileges, users can browse through directories that their own permissions would not allow.

This policy does not affect installations that run in the user's security context. Also, see the "Disable browse dialog box for new source" policy (Microsoft Developer's Network, 2000).

***Enable user to use media source while elevated***

Allows users to install programs from removable media, such as floppy disks and CD-ROMs, during privileged installations.

This policy permits all users to install programs from removable media, even when the installation program is running with elevated system privileges. By default, users can install programs from removable media only when the installation runs in the user's security context. During privileged installations, such as those offered on the desktop or displayed in Add/Remove Programs, only system administrators can install from removable media.

This policy does not affect installations that run in the user's security context. By default, users can install

from removable media when the installation runs in their own security context (Microsoft Developer's Network, 2000).

***Enable user to patch elevated products***

Allows users to upgrade programs during privileged installations.

This policy permits all users to install patches, even when the installation program is running with elevated system privileges. Patches are updates or upgrades that replace only those program files that have changed. Because patches can easily be vehicles for malicious programs, some installations prohibit their use.

By default, only system administrators can apply patches during installations with elevated privileges, such as installations offered on the desktop or displayed in Add/Remove Programs.

This policy does not affect installations that run in the user's security context. By default, users can install patches to programs that run in their own security context. Also, see the "Disable patching" policy (Microsoft Developer's Network, 2000).

***Allow admin to install from terminal services session***

Allows Terminal Services administrators to install and configure programs remotely.

By default, system administrators can install programs only when system administrators are logged on to the computer on which the program is being installed. This policy creates a special exception for computers running Terminal Services.

This policy affects system administrators only. Other users cannot install programs remotely (Microsoft Developer's Network, 2000).

***Cache transforms in secure location on workstation***

Saves copies of transform files in a secure location on the local computer.

Transform files consist of instructions to modify or customize a program during installation. By default, Windows Installer stores transform files in the Application Data directory in the user's profile. When a user reinstalls, removes, or repairs an installation, the transform file is available, even if the user is on a different computer or isn't connected to the network.

If you enable this policy, the transform file is saved in a secure location on the user's computer instead of in the user profile. Because Windows Installer requires the transform file in order to repeat an installation in which the transform file was used, the user must be using the same computer or be connected to the original or identical media to reinstall, remove, or repair the installation.

This policy is designed for enterprises that must take special precautions to prevent unauthorized or malicious editing of transform files (Microsoft Developer's Network, 2000).

### ***Logging***

Specifies the types of events that Windows Installer records in its transaction log for each installation. The log, Msi.log, appears in the Temp directory of the system volume.

When you enable this policy, you can specify the types of events you want Windows Installer to record. To indicate that an event type is recorded, type the letter representing the event type. You can type the letters in any order and list as many or as few event types as you desire.

To disable logging, delete all of the letters from the box.

If you disable this policy or do not configure it, Windows Installer logs the default event types, represented by the letters "iweap" (Microsoft Developer's Network, 2000).

## **System**

### ***Remove security option from start menu***

Removes the Windows Security item from the Settings menu on Terminal Services clients.

If you enable this policy, the Windows Security item does not appear in Settings menu on the Start menu. As a result, users must type a security attention sequence, such as Ctrl+Alt+End, to open the Windows Security dialog box on a Terminal Services client.

This policy is designed to prevent inexperienced users from logging on to Terminal Services inadvertently (Microsoft Developer's Network, 2000).

### ***Remove disconnect item from start menu***

Removes the Disconnect item from the Shut Down Windows dialog box on Terminal Services clients.

If you enable this policy, the Disconnect item does not appear in the drop-down list of options in the Shut Down Windows dialog box. As a result, Terminal Services users cannot use this

familiar method to disconnect their client from a Terminal Services server.

This policy affects the Shut Down Windows dialog box only. It does not prevent users from using other methods of disconnecting from a Terminal Services server (Microsoft Developer's Network, 2000).

### ***Disable Boot / Shutdown / Logon / Logoff status messages***

Suppresses system status messages.

If you enable this policy, the system does not display a message reminding users to wait while their system starts or shuts down, or while users log on or off (Microsoft Developer's Network, 2000).

### ***Verbose vs. normal status messages***

Directs the system to display highly detailed status messages.

If you enable this policy, the system displays status message that reflect each step in the process of starting, shutting down, logging on or logging off the system.

This policy is designed for sophisticated users that require this information.

Note: This policy is ignored if the "Disable Boot / Shutdown / Logon / Logoff status messages" policy is enabled (Microsoft Developer's Network, 2000).

### ***Display autoplay***

Disables the Autoplay feature.

Autoplay begins reading from a drive as soon as you insert media in the drive. As a result, the setup file of programs and the music on audio media starts immediately.

By default, Autoplay is disabled on removable drives, such as the floppy disk drive (but not the CD-ROM drive), and on network drives.

If you enable this policy, you can also disable Autoplay on CD-ROM drives, or disable Autoplay on all drives.

This policy disables Autoplay on additional types of drives. You cannot use this policy to enable Autoplay on drives on which it is disabled by default.

Note: This policy appears in both the Computer Configuration and User Configuration folders. If the settings conflict, the setting in Computer Configuration takes precedence over the setting in User Configuration (Microsoft Developer's Network, 2000).

### ***Don't display welcome screen at logon***

Suppresses the "Getting Started with Windows 2000" welcome screen.

This policy hides the welcome screen that is displayed on Windows 2000 Professional each time the user logs on.

Users can still display the "Getting Started with Windows 2000" welcome screen by selecting it from the Start menu or by typing "Welcome" in the Run dialog box.

This policy applies only to Windows 2000 Professional. It does not affect the "Configure Your Server on a Windows 2000 Server" screen on Windows 2000 Server.

Note: This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Tip: To display the welcome screen, click Start, point to Programs, point to Accessories, point to System Tools, and then click "Getting Started." To suppress the welcome screen without setting a policy, clear the "Show this screen at startup" check box on the welcome screen (Microsoft Developer's Network, 2000).

### ***Run these programs at user logon***

Specifies additional programs or documents that Windows starts automatically when a user logs on to the system.

To use this policy, click Show, click Add and, in the text box, type the name of the executable program (.exe) file or document file. Unless the file is located in the %Systemroot% directory, you must specify the fully qualified path to the file.

Note: This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the system starts the programs specified in the Computer Configuration policy just before it starts the programs specified in the User Configuration policy (Microsoft Developer's Network, 2000).

### ***Disable the run once list***

Ignores customized run-once lists.

You can create a customized list of additional programs and documents that are started automatically the next time the system starts (but not thereafter). These programs are added to the standard list of programs and services that the system starts.

If you enable this policy, the system ignores the run-once list.

If you disable this policy, or do not configure it, the system runs the programs in the run-once list.

This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.



Tip: Customized run-once lists are stored in the registry in HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce (Microsoft Developer's Network, 2000).

### ***Disable legacy run list***

Ignores the customized run list for Windows NT 4.0 and earlier.

On Windows 2000 and Windows NT 4.0 and earlier, you can create a customized list of additional programs and documents that the system starts automatically when it starts. These programs are added to the standard run list of programs and services that the system starts.

If you disable this policy, or do not configure it, Windows 2000 adds any customized run list configured for Windows NT 4.0 and earlier to its run list.

If you enable this policy, the system ignores the run list for Windows NT 4.0 and earlier.

This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Tip: To create a customized run list by using a policy, use the "Run these applications at startup" policy.

The customized run lists for Windows NT 4.0 and earlier are stored in the registry in HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run and HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run. These can be configured by using the "Run" policy in System Policy Editor for Windows NT 4.0 and earlier (Microsoft Developer's Network, 2000).

### ***Do not automatically encrypt files moved to encrypted folders***

Prevents Windows Explorer from encrypting files that are moved to an encrypted folder.

If you disable this policy or do not configure it, Windows Explorer automatically encrypts files that are moved to an encrypted folder.

This policy applies only to files moved within a volume. When files are moved to other volumes, or if you create a new file in an encrypted folder, Windows Explorer encrypts those files automatically (Microsoft Developer's Network, 2000).

### ***Download missing COM components***

Directs the system to search Active Directory for missing Component Object Model (COM) components that a program requires.

Many Windows programs, such as the MMC snap-ins, use the interfaces provided by the COM. These programs cannot perform all of their functions unless Windows 2000 has internally registered the required components.

If you enable this policy and a component registration is missing, the system searches for it in Active Directory and if it is found, downloads it. The resulting searches might make some programs start or run slowly.

If you disable this policy or do not configure it, the program continues without the registration. As a result, the program might not perform all of its functions, or it might stop.

This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration (Microsoft Developer's Network, 2000).

## ***Logon***

### ***Run logon scripts synchronously***

Directs the system to wait for the logon scripts to finish running before it starts the Windows Explorer interface program and creates the desktop.

If you enable this policy, Windows Explorer does not start until the logon scripts have finished running. This setting assures that logon script processing is complete before the user starts working, but it can delay the appearance of the desktop.

If you disable this policy or do not configure it, the logon scripts and Windows Explorer are not synchronized and can run simultaneously.

This policy appears in the Computer Configuration and User Configuration folders. The policy set in Computer Configuration takes precedence over the policy set in User Configuration (Microsoft Developer's Network, 2000).

### ***Run startup scripts asynchronously***

Lets the system run startup scripts simultaneously.

Startup scripts are batch files that run before the user is invited to log on. By default, the system waits for each startup script to complete before it runs the next startup script.

If you enable this policy, the system does not coordinate the running of startup scripts. As a result, startup scripts can run simultaneously.

If you disable this policy or do not configure it, a startup cannot run until the previous script is complete (Microsoft Developer's Network, 2000).

### ***Run startup scripts visible***

Displays the instructions in startup scripts as they run.

Startup scripts are batch files of instructions that run before the user is invited to log on. By default, the system does not display the instructions in the startup script.

If you enable this policy, the system displays each instruction in the startup script as it runs. The instructions appear in a command window. This setting is designed for advanced users.

If you disable this policy or do not configure it, the instructions are suppressed (Microsoft Developer's Network, 2000).

### ***Run Shutdown scripts visible***

Displays the instructions in shutdown scripts as they run.

Shutdown scripts are batch files of instructions that run when the user restarts the system or shuts it down. By default, the system does not display the instructions in the shutdown script.

If you enable this policy, the system displays each instruction in the shutdown script as it runs. The instructions appear in a command window.

If you disable this policy or do not configure it, the instructions are suppressed (Microsoft Developer's Network, 2000).

### ***Maximum wait time for group policy scripts***

This policy limits the total time allowed for all logon, startup, and shutdown scripts applied by Group Policy to finish running. If the scripts have not finished running when the specified time expires, the system stops script processing and records an error event.

By default, the system lets the combined set of scripts run for up to 600 seconds (10 minutes), but you can use this policy to adjust this interval.

To use this policy, in the Seconds box, type a number from 1 to 32,000 for the number of seconds you want the system to wait for the set of scripts to finish. To direct the system to wait until the scripts have finished, no matter how long they take, type 0.

This interval is particularly important when other system tasks must wait while the scripts complete. By default, each startup script must complete before the next one runs. Also, you can use the "Run logon scripts

synchronously" policy to direct the system to wait for the logon scripts to complete before loading the desktop.

An excessively long interval can delay the system and inconvenience users. However, if the interval is too short, prerequisite tasks might not be done, and the system can appear to be ready prematurely (Microsoft Developer's Network, 2000).

### ***Delete cached copies of roaming profiles***

Determines whether the system saves a copy of a user's roaming profile on the local computer's hard drive when the user logs off.

This policy and related policies in this folder describe a strategy for managing user profiles residing on remote servers. In particular, they tell the system how to respond when a remote profile is slow to load.

Roaming profiles reside on a network server. By default, when users with roaming profiles log off, the system also saves a copy of their roaming profile on the hard drive of the computer they are using in case the server that stores the roaming profile is unavailable when the user logs on again. The local copy is also used when the remote copy of the roaming user profile is slow to load.

If you enable this policy, any local copies of the user's roaming profile are deleted when the user logs off. The roaming profile still remains on the network server that stores it.

Important: Do not enable this policy if you are using the slow link detection feature of Windows 2000. To respond to a slow link, the system requires a local copy of the user's roaming profile (Microsoft Developer's Network, 2000).

### ***Do not detect slow network connections***

Disables the slow link detection feature.

Slow link detection measures the speed of the connection between a user's computer and the remote server that stores the roaming user profile. When the system detects a slow link, the related policies in this folder tell the system how to respond.

If you enable this policy, the system does not detect slow connections or recognize any connections as being slow. As a result, the system does not respond to slow connections to user profiles and it ignores the policies that tell the system how to respond to a slow connection.

If you disable this policy or do not configure it, slow link detection is enabled. The system measures the

speed of the connection between the user's computer and profile server. If the connection is slow (as defined by the "Slow network connection timeout for user profiles" policy), the system applies the other policies set in this folder to determine how to proceed. By default, when the connection is slow, the system loads the local copy of the user profile (Microsoft Developer's Network, 2000).

### ***Slow network connection time out for user profiles***

Defines a slow connection for roaming user profiles.

If the server on which the user's roaming user profile resides takes longer to respond than the thresholds set by this policy allow, then the system considers the connection to the profile to be slow.

This policy and related policies in this folder together define the system's response when roaming user profiles are slow to load.

This policy establishes thresholds for two tests. For computers connected to IP networks, the system measures the rate at which the remote server returns data in response to an IP ping message. To set a threshold for this test, in the Connection speed box, type a decimal number between 0 and 4,294,967,200, representing the minimum acceptable transfer rate in kilobits per second. By default, if the server returns fewer than 500 kilobits of data per second, it is considered to be slow.

For non-IP computers, the system measures the responsiveness of the remote server's file system. To set a threshold for this test, in the Time box, type a decimal number between 0 and 20,000, representing the maximum acceptable delay, in milliseconds. By default, if the server's file system does not respond within 120 milliseconds, it is considered to be slow.

Consider increasing this value for clients using DHCP Service-assigned addresses or for computers accessing profiles across dial-up connections.

Important: If the "Do not detect slow network connections" policy is enabled, this policy is ignored. Also, if the "Delete cached copies of roaming profiles" policy is enabled, there is no local copy of the roaming profile to load when the system detects a slow connection (Microsoft Developer's Network, 2000).

### ***Wait for remote user profile***

Directs the system to wait for the remote copy of the roaming user profile to load, even when loading is slow. Also, the system waits for the remote copy when the user is notified about a slow connection, but does not respond in the time allowed.

This policy and related policies in this folder together define the system's response when roaming user profiles are slow to load.

If you disable this policy or do not configure it, then when a remote profile is slow to load, the system loads the local copy of the roaming user profile. The local copy is also used when the user is consulted (as set in the "Prompt user when slow link is detected" policy), but does not respond in the time allowed (as set in the "Timeout for dialog boxes" policy).

Waiting for the remote profile is appropriate when users move between computers frequently and the local copy of their profile is not always current. Using the local copy is desirable when quick logging on is a priority.

Important: If the "Do not detect slow network connections" policy is enabled, this policy is ignored. Also, if the "Delete cached copies of roaming profiles" policy is enabled, there is no local copy of the roaming profile to load when the system detects a slow connection (Microsoft Developer's Network, 2000).

### ***Prompt user when slow link is detected***

Notifies users when their roaming profile is slow to load. The notice lets users decide whether to use a local copy or to wait for the roaming user profile.

If you disable this policy or do not configure it, when a roaming user profile is slow to load, the system does not consult the user. Instead, it loads the local copy of the profile. If you have enabled the "Wait for remote user profile" policy, then the system loads the remote copy without consulting the user.

This policy and related policies in this folder together define the system's response when roaming user profiles are slow to load.

To adjust the time within which the user must respond to this notice, use the "Timeout for dialog boxes" policy.

Important: If the "Do not detect slow network connections" policy is enabled, this policy is ignored. Also, if the "Delete cached copies of roaming profiles" policy is enabled, there is no local copy of the roaming profile to

load when the system detects a slow connection (Microsoft Developer's Network, 2000).

### ***Timeout for dialog boxes***

Determines how long the system waits for a user response before it uses a default value.

The default value is applied when the user does not respond to messages explaining that any of the following events has occurred:

- The system detects a slow connection between the user's computer and the server that stores users' roaming user profiles.

- The system cannot access users' server-based profiles when users log on or off.

- Users' local profiles are newer than their server-based profiles.

You can use this policy to override the system's default value of 30 seconds. To use this policy, type a decimal number between 0 and 600 for the length of the interval (Microsoft Developer's Network, 2000).

### ***Log users off when roaming profile fails***

Logs a user off automatically when the system cannot load the user's roaming user profile.

This policy is used when the system cannot find the roaming user profile or the profile contains errors which prevent it from loading correctly.

If you disable this policy or do not configure it, when the roaming profile fails, the system loads a local copy of the roaming user profile, if one is available. Otherwise, the system loads the default user profile (stored in %Systemroot%\Documents and Settings\Default User).

Also, see the "Delete cached copies of roaming profiles" policy (Microsoft Developer's Network, 2000).

### ***Maximum retries to unload and update user profile***

Determines how many times the system tries to unload and update the registry portion of a user profile. When the number of trials specified by this policy is exhausted, the system stops trying. As a result, the user profile might not be current, and local and roaming user profiles might not match.

When a user logs off of the computer, the system unloads the user-specific section of the registry (HKEY\_CURRENT\_USER) into a file (NTUSER.DAT) and updates it. However, if another program or service is reading or editing the registry, the system cannot unload it.

The system tries repeatedly (at a rate of once per second) to unload and update the registry settings. By default, the system repeats its periodic attempts 60 times (over the course of one minute).

If you enable this policy, you can adjust the number of times the system tries to unload and update the user's registry settings. (You cannot adjust the retry rate.)

If you disable this policy or do not configure it, the system repeats its attempt 60 times.

If you set the number of retries to 0, the system tries just once to unload and update the user's registry settings. It does not try again.

Note: This policy is particularly important to servers running Terminal Services. Because Terminal Services edits the user's registry settings when they log off, the system's first few attempts to unload the user settings are more likely to fail.

This policy does not affect the system's attempts to update the files in the user profile.

Tip: Consider increasing the number of retries specified in this policy if there are many user profiles stored in the computer's memory. This indicates that the system has not been able to unload the profile (Microsoft Developer's Network, 2000).

## ***Disk Quotas***

### ***Enable disk quotas***

Enables and disables disk quota management on all NTFS volumes of the computer, and prevents users from changing the setting.

If you enable this policy, disk quota management is enabled, and users cannot disable it.

If you disable the policy, disk quota management is disabled, and users cannot enable it.

If this policy is not configured, disk quota management is disabled by default, but administrators can enable it.

To prevent users from changing the setting while a policy is in effect, the system disables the "Enable quota management" option on the Quota tab of NTFS volumes.

Note: This policy enables disk quota management but does not establish or enforce a particular disk quota limit. To specify a disk quota limit, use the "Default quota limit and warning level" policy. Otherwise, the system uses the physical space on the volume as the quota limit.



Tip: To enable or disable disk quota management without setting a policy, in My Computer, right-click the name of an NTFS volume, click Properties, click the Quota tab, and then click the "Enable quota management" option (Microsoft Developer's Network, 2000).

### ***Enforce disk quota limit***

Determines whether disk quota limits are enforced and prevents users from changing the setting.

If you enable this policy, disk quota limits are enforced. If you disable this policy, disk quota limits are not enforced. When you enable or disable the policy, the system disables the "Deny disk space to users exceeding quota limit" option on the Quota tab so administrators cannot change the setting while a policy is in effect.

If the policy is not configured, the disk quota limit is not enforced by default, but administrators change the setting.

Enforcement is optional. When users reach an enforced disk quota limit, the system responds as though the physical space on the volume were exhausted. When users reach an unenforced limit, their status in the Quota Entries window changes, but they can continue to write to the volume as long as physical space is available.

Note: This policy overrides user settings that enable or disable quota enforcement on their volumes.

Tip: To specify a disk quota limit, use the "Default quota limit and warning level" policy. Otherwise, the system uses the physical space on the volume as the quota limit (Microsoft Developer's Network, 2000).

### ***Default quota limit and warning level***

Specifies the default disk quota limit and warning level for new users of the volume.

This policy determines how much disk space can be used by each user on each of the NTFS file system volumes on a computer. It also specifies the warning level, the point at which the user's status in the Quota Entries window changes to indicate that the user is approaching the disk quota limit.

This policy overrides new users' settings for the disk quota limit and warning level on their volumes, and it disables the corresponding options in the "Select the default quota limit for new users of this volume" section on the Quota tab.

This policy applies to all new users as soon as they write to the volume. It does not affect disk quota limits for

current users or affect customized limits and warning levels set for particular users (on the Quota tab in Volume Properties).

If you disable this policy or do not configure it, the disk space available to users is not limited. The disk quota management feature uses the physical space on each volume as its quota limit and warning level.

When you select a limit, remember that the same limit applies to all users on all volumes, regardless of actual volume size. Be sure to set the limit and warning level so that it is reasonable for the range of volumes in the group.

This policy is effective only when disk quota management is enabled on the volume. Also, if disk quotas are not enforced, users can exceed the quota limit you set. When users reach the quota limit, their status in the Quota Entries window changes, but users can continue to write to the volume (Microsoft Developer's Network, 2000).

### ***Log event when quota limit exceeded***

Determines whether the system records an event in the local Application log when users reach their disk quota limit on a volume, and prevents users from changing the logging setting.

If you enable this policy, the system records an event when the user reaches their limit. If you disable this policy, no event is recorded. Also, when you enable or disable this policy, the system disables the "Log event when a user exceeds their quota limit" option on the Quota tab so administrators cannot change the setting while a policy is in effect.

If the policy is not configured, no events are recorded, but administrators can use the Quota tab option to change the setting.

This policy is independent of the enforcement policies for disk quotas. As a result, you can direct the system to log an event regardless of whether or not you choose to enforce the disk quota limit.

Also, this policy does not affect the Quota Entries window on the Quota tab. Even without the logged event, users can detect that they have reached their limit because their status in the Quota Entries window changes.

Tip: To find the logging option, in My Computer, right-click the name of an NTFS file system volume, click Properties, and then click the Quota tab (Microsoft Developer's Network, 2000).

### ***Log event when quota- warning level exceeded***

Determines whether the system records an event in the Application log when users reach their disk quota warning level on a volume.

If you enable this policy, the system records an event. If you disable this policy, no event is recorded. When you enable or disable the policy, the system disables the corresponding "Log event when a user exceeds their warning level" option on the Quota tab, so that administrators cannot change the logging setting while a policy is in effect.

If the policy is not configured, no event is recorded, but administrators can use the Quota tab option to change the logging setting.

This policy does not affect the Quota Entries window on the Quota tab. Even without the logged event, users can detect that they have reached their warning level because their status in the Quota Entries window changes.

Tip: To find the logging option, in My Computer, right-click the name of an NTFS file system volume, click Properties, and then click the Quota tab (Microsoft Developer's Network, 2000).

### ***Apply policy to removable media***

Extends the disk quota policies in this folder to NTFS file system volumes on removable media.

If you disable this policy or do not configure it, the disk quota policies established in this folder apply to fixed-media NTFS volumes only (Microsoft Developer's Network, 2000).

## ***DNS Client***

### ***Primary DNS suffix***

Specifies the primary Domain Name System (DNS) suffix for all affected computers. The primary DNS suffix is used in DNS name registration and DNS name resolution.

This policy lets you specify a primary DNS suffix for a group of computers, and prevents users, including administrators, from changing it.

If you disable this policy or do not configure it, each computer uses its local primary DNS suffix, which is usually the DNS name of Active Directory domain to which it is joined. However, administrators can use System in Control Panel to change the primary DNS suffix of a computer.

To use this policy, in the text box provided, type the entire primary DNS suffix you want to assign. For example, microsoft.com.

This policy does not disable the DNS Suffix and NetBIOS Computer Name dialog box that administrators use to change the primary DNS suffix of a computer. However, if administrators enter a suffix, that suffix is ignored while this policy is enabled.

Important: To make changes to this policy effective, you must restart Windows 2000 on all computers affected by the policy.

Note: This policy has no effect on domain controllers.

Tip: To change the primary DNS suffix of a computer without setting a policy, click System in Control Panel, click the Network Identification tab, click Properties, click More, and then enter a suffix in the "Primary DNS suffix of this computer" box (Microsoft Developer's Network, 2000).

### ***Group Policies***

#### ***Disable background refresh of group policy***

Prevents Group Policy from being updated while the computer is in use. This policy applies to Group Policies for computers, users, and domain controllers.

If you enable this policy, the system waits until the current user logs off the system before updating the computer and user policies.

If you disable this policy, updates can be applied while users are working. The frequency of updates is determined by the "Group Policy refresh interval for computers" and "Group Policy refresh interval for users" policies (Microsoft Developer's Network, 2000).

#### ***Apply group policy for computers asynchronously during startup***

Lets the system display the logon prompt before it finishes updating computer Group Policy.

If you enable this policy, the system does not wait for Group Policy updates to complete before inviting the user to log on. As a result, the Windows interface might appear to be ready before computer Group Policy is applied.

If you disable this policy or do not configure it, users cannot log on until computer Group Policy is updated (Microsoft Developer's Network, 2000).

### ***Apply group policy for users asynchronously during logon***

Lets the system display the Windows desktop before it finishes updating user Group Policy.

If you enable this policy, the system does not coordinate the tasks of loading desktop and updating user Group Policy. As a result, Windows might appear ready for use before user Group Policy is updated.

If you disable this policy or do not configure it, the system does not make the desktop available to users until user Group Policy is updated (Microsoft Developer's Network, 2000).

### ***Group policy refresh interval for computers***

Specifies how often Group Policy for computers is updated while the computer is in use (in the background). This policy specifies a background update rate only for Group Policies in the Computer Configuration folder.

In addition to background updates, Group Policy for the computer is always updated when the system starts.

By default, computer Group Policy is updated in the background every 90 minutes, with a random offset of 0 to 30 minutes.

You can specify an update rate from 0 to 64,800 minutes (45 days). If you select 0 minutes, the computer tries to update Group Policy every 7 seconds. However, because updates might interfere with users' work and increase network traffic, very short update intervals are not appropriate for most installations.

If you disable this policy, Group Policy is updated every 90 minutes (the default). To specify that Group Policy should never be updated while the computer is in use, select the "Disable background refresh of Group Policy" policy.

The Group Policy refresh interval for computers policy also lets you specify how much the actual update interval varies. To prevent clients with the same update interval from requesting updates simultaneously, the system varies the update interval for each client by a random number of minutes. The number you type in the random time box sets the upper limit for the range of variance. For example, if you type 30 minutes, the system selects a variance of 0 to 30 minutes. Typing a large number establishes a broad range and makes it less likely that client requests overlap. However, updates might be delayed significantly.

This policy establishes the update rate for computer Group Policy. To set an update rate for user policies, use the "Group Policy refresh interval for users" policy (located in User Configuration\Administrative Templates\System\Group Policy).

This policy is only used when the "Disable background refresh of Group Policy" policy is not enabled.

Note: Consider notifying users that their policy is updated periodically so that they recognize the signs of a policy update. When Group Policy is updated, the Windows desktop is refreshed; it flickers briefly and closes open menus. Also, restrictions imposed by Group Policies, such as those that limit the programs users can run, might interfere with tasks in progress (Microsoft Developer's Network, 2000).

### ***Group policy refresh interval for domain controllers***

Specifies how often Group Policy is updated on domain controllers while they are running (in the background). The updates specified by this policy occur in addition to updates performed when the system starts.

By default, Group Policy on the domain controllers is updated every five minutes.

You can specify an update rate from 0 to 64,800 minutes (45 days). If you select 0 minutes, the domain controller tries to update Group Policy every 7 seconds. However, because updates might interfere with users' work and increase network traffic, very short update intervals are not appropriate for most installations.

If you disable this policy, the domain controller updates Group Policy every 5 minutes (the default). To specify that Group Policies for users should never be updated while the computer is in use, select the "Disable background refresh of Group Policy" policy.

This policy also lets you specify how much the actual update interval varies. To prevent domain controllers with the same update interval from requesting updates simultaneously, the system varies the update interval for each controller by a random number of minutes. The number you type in the random time box sets the upper limit for the range of variance. For example, if you type 30 minutes, the system selects a variance of 0 to 30 minutes. Typing a large number establishes a broad range and makes it less likely that update requests overlap. However, updates might be delayed significantly.

Note: This policy is used only when you are establishing policy for a domain, site, organizational unit (OU), or customized group. If you are establishing policy for a local computer only, the system ignores this policy (Microsoft Developer's Network, 2000).

### ***User group policy loopback processing mode***

Applies alternate user policies when a user logs on to a computer affected by this policy.

This policy directs the system to apply the set of Group Policy objects for the computer to any user who logs on to a computer affected by this policy. It is intended for special-use computers, such as those in public places, laboratories, and classrooms, where you must modify the user policy based on the computer that is being used.

By default, the user's Group Policy objects determine which user policies apply. If this policy is enabled, then, when a user logs on to this computer, the computer's Group Policy objects determine which set of Group Policy objects applies.

To use this policy, select one of the following policy modes from the Mode box:

- "Replace" indicates that the user policies defined in the computer's Group Policy objects replace the user policies normally applied to the user.

- "Merge" indicates that the user policies defined in the computer's Group Policy objects and the user policies normally applied to the user are combined. If the policy settings conflict, the user policies in the computer's Group Policy objects take precedence over the user's normal policies.

If you disable this policy or do not configure it, the user's Group Policy objects determines which user policies apply.

Note: This policy is effective only when both the computer account and the user account are in Windows 2000 domains (Microsoft Developer's Network, 2000).

### ***Group policy slow link detection***

Defines a slow connection for purposes of applying and updating Group Policy.

If the rate at which data is transferred from the domain controller providing a policy update to the computers in this group is slower than the rate specified by this policy, the system considers the connection to be slow.

The system's response to a slow policy connection varies among policies. The program implementing the policy can specify the response to a slow link. Also, the policy processing policies in this folder let you override the programs' specified responses to slow links.

To use this policy, in the "Connection speed" box, type a decimal number between 0 and 4,294,967,200 (0xFFFFFFFF), indicating a transfer rate in kilobits per second. Any connection slower than this rate is considered to be slow. If you type 0, all connections are considered to be fast.

If you disable this policy or do not configure it, the system uses the default value of 500 kilobits per second.

This policy appears in the Computer Configuration and User Configuration folders. The policy in Computer Configuration defines a slow link for policies in the Computer Configuration folder. The policy in User Configuration defines a slow link for policies in the User Configuration folder (Microsoft Developer's Network, 2000).

### ***Registry policy processing***

Determines when registry policies are updated.

This policy affects all policies in the Administrative Templates folder and any other policies that store values in the registry.

It overrides customized settings that the program implementing a registry policy set when it was installed.

If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.

The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data.

The "Process even if the Group Policy objects have not changed" option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it (Microsoft Developer's Network, 2000).

### ***IE maintenance policy processing***



Determines when Internet Explorer Maintenance policies are updated.

This policy affects all policies that use the Internet Explorer Maintenance component of Group Policy, such as those in Windows Settings\Internet Explorer Maintenance.

It overrides customized settings that the program implementing the Internet Explorer Maintenance policy set when it was installed.

If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.

The "Allow processing across a slow network connection" option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.

The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data.

The "Process even if the Group Policy objects have not changed" option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it (Microsoft Developer's Network, 2000).

### ***Software installation policy processing***

Determines when software installation policies are updated.

This policy affects all policies that use the software installation component of Group Policy, such as policies in Software Settings\Software Installation. You can set software installation policy only for Group Policy objects stored in Active Directory, not for Group Policy objects on the local computer.

This policy overrides customized settings that the program implementing the software installation policy set when it was installed.

If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.

The "Allow processing across a slow network connection" option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.

The "Process even if the Group Policy objects have not changed" option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it (Microsoft Developer's Network, 2000).

### ***Folder redirection policy processing***

Determines when folder redirection policies are updated.

This policy affects all policies that use the folder redirection component of Group Policy, such as those in WindowsSettings\Folder Redirection. You can only set folder redirection policy for Group Policy objects, stored in Active Directory, not for Group Policy objects on the local computer.

This policy overrides customized settings that the program implementing the folder redirection policy set when it was installed.

If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.

The "Allow processing across a slow network connection" option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.

The "Process even if the Group Policy objects have not changed" option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it (Microsoft Developer's Network, 2000).

### ***Scripts policy processing***

Determines when policies that assign shared scripts are updated.

This policy affects all policies that use the scripts component of Group Policy, such as those in WindowsSettings\Scripts.

It overrides customized settings that the program implementing the scripts policy set when it was installed.

If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.

The "Allow processing across a slow network connection" option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.

The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data.

The "Process even if the Group Policy objects have not changed" option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it (Microsoft Developer's Network, 2000).

### ***Security policy processing***

Determines when security policies are updated.

This policy affects all policies that use the security component of Group Policy, such as those in Windows Settings\Security Settings.

It overrides customized settings that the program implementing the security policy set when it was installed.

If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.

The "Allow processing across a slow network connection" option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.

The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data.

The "Process even if the Group Policy objects have not changed" option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it (Microsoft Developer's Network, 2000).

### ***IP security policy processing***

Determines when IP security policies are updated.

This policy affects all policies that use the IP security component of Group Policy, such as policies in Computer Configuration\Windows Settings\Security Settings\IP Security Policies on Local Machine.

It overrides customized settings that the program implementing the IP security policy set when it was installed.

If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.

The "Allow processing across a slow network connection" option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.

The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data.

The "Process even if the Group Policy objects have not changed" option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it (Microsoft Developer's Network, 2000).

### ***EFS recovery policy processing***

Determines when encryption policies are updated.

This policy affects all policies that use the encryption component of Group Policy, such as policies related to encryption in Windows Settings\Security Settings.

It overrides customized settings that the program implementing the encryption policy set when it was installed.

If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.

The "Allow processing across a slow network connection" option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.

The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a program to stop or operate abnormally, and, in rare cases, damage data.

The "Process even if the Group Policy objects have not changed" option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it (Microsoft Developer's Network, 2000).

### ***Disk quota policy processing***

Determines when disk quota policies are updated.

This policy affects all policies that use the disk quota component of Group Policy, such as those in Computer Configuration\Administrative Templates\System\File System\Disk Quotas.

It overrides customized settings that the program implementing the disk quota policy set when it was installed.

If you enable this policy, you can use the check boxes provided to change the options. If you disable this policy or do not configure it, it has no effect on the system.

The "Allow processing across a slow network connection" option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.

The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. Background updates can disrupt the user, cause a

program to stop or operate abnormally, and, in rare cases, damage data.

The "Process even if the Group Policy objects have not changed" option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that they are updated only when changed. However, you might want to update unchanged policies, such as reapplying a desired setting in case a user has changed it (Microsoft Developer's Network, 2000).

### ***Windows File Protection***

#### ***Set Windows file protection scanning***

Determines when Windows File Protection scans protected files. This policy directs Windows File Protection to enumerate and scan all system files for changes.

You can use this policy to direct Windows File Protection to scan files more often. By default, files are scanned only during setup.

To use this policy, enable the policy and select a rate from the "Scanning Frequency" box.

- "Do not scan during startup," the default, scans files only during setup.

- "Scan during startup" also scans files each time you start Windows 2000. This setting delays each startup.

- "Scan once" scans files the next time you start the system.

Note: This policy affects file scanning only. It does not affect the standard background file change detection that Windows File Protection provides (Microsoft Developer's Network, 2000).

#### ***Hide the file scan process window***

Hides the file scan progress window.

This window provides status information to sophisticated users, but might confuse novices.

If you enable this policy, the file scan window does not appear during file scanning.

If you disable this policy or do not configure it, the file scan progress window appears (Microsoft Developer's Network, 2000).

#### ***Limit Windows file protection cache size***

Specifies the maximum amount of disk space that can be used for the Windows File Protection file cache.

Windows File Protection adds protected files to the cache until the cache content reaches the quota. If the quota is greater than 50 MB, WFP adds other important Windows

2000 files to the cache until the cache size reaches the quota.

To use this policy, enable the policy, and enter the maximum amount of disk space to be used (in MB). To indicate that the cache size is unlimited, select "4294967295" as the maximum amount of disk space.

If you disable this policy or do not configure it, the default value is set to 50 MB on Windows 2000 Professional and is unlimited (4294967295 MB) on Windows 2000 Server (Microsoft Developer's Network, 2000).

### ***Specify Windows file protection cache location***

Specifies an alternate location for the Windows File Protection cache.

To use the policy, enable the policy, and enter the fully qualified local path to the new location in the "Cache file path" box.

If you disable this policy or do not configure it, the Windows File Protection cache is located in the %Systemroot%\System32\Dllcache directory.

Note: Do not put the cache on a network shared directory (Microsoft Developer's Network, 2000).

## **Network**

### ***Offline Files***

#### ***Enabled***

Determines whether the Offline Files feature is enabled.

This policy also disables the "Enable Offline Files" option on the Offline Files tab. This prevents users from trying to change the option while a policy controls it.

Offline Files saves a copy of network files on the user's computer for use when the computer is not connected to the network.

If you enable this policy, Offline Files is enabled and users cannot disable it.

If you disable this policy, Offline Files is disabled and users cannot enable it.

By default, Offline Files is enabled on Windows 2000 Professional and is disabled on Windows 2000 Server.

Tip: To enable Offline Files without setting a policy, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then click "Enable Offline Files."

Note: To make changes to this policy effective, you must restart Windows 2000 (Microsoft Developer's Network, 2000).

### ***Disable user configuration of offline files***

Prevents users from enabling, disabling, or changing the configuration of Offline Files.

This policy removes the Offline Files tab from the Folder Options dialog box. It also removes the Settings item from the Offline Files context menu and disables the Settings button on the Offline Files Status dialog box. As a result, users cannot view or change the options on the Offline Files tab or Offline Files dialog box.

This is a comprehensive policy that locks down the configuration you establish by using other policies in this folder.

This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Tip: This policy provides a quick method for locking down the default settings for Offline Files. To accept the defaults, just enable this policy. You do not have to disable any other policies in this folder (Microsoft Developer's Network, 2000).

### ***Synchronize all offline files before logging off***

Determines whether offline files are fully synchronized when users log off.

This policy also disables the "Synchronize all offline files before logging off" option on the Offline Files tab. This prevents users from trying to change the option while a policy controls it.

If you enable this policy, offline files are fully synchronized. Full synchronization ensures that offline files are complete and current.

If you disable this policy, the system only performs a quick synchronization. Quick synchronization ensures that files are complete, but does not ensure that they are current.

If you do not configure this policy, the system performs a quick synchronization by default, but users can change this option.

This policy appears in the Computer Configuration and User Configuration folders. If both policies are



configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Tip: To change the synchronization method without setting a policy, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then select the "Synchronize all offline files before logging off" option (Microsoft Developer's Network, 2000).

### ***Default cache size***

Limits the percentage of the computer's disk space that can be used to store automatically-cached offline files.

This policy also disables the "Amount of disk space to use for temporary offline files" option on the Offline Files tab. This prevents users from trying to change the option while a policy controls it.

Automatic caching can be set on any network share. When a user opens a file on the share, the system automatically stores a copy of the file on the user's computer.

This policy does not limit the disk space available for files that user's make available offline manually.

If you enable this policy, you can specify an automatic-cache disk space limit.

If you disable this policy, the system limits the space that automatically-cached files occupy to 10 percent of the space on the system drive (Microsoft Developer's Network, 2000).

### ***Action on server disconnect***

Determines whether network files remain available if the computer is suddenly disconnected from the server hosting the files.

This policy also disables the "When a network connection is lost" option on the Offline Files tab. This prevents users from trying to change the option while a policy controls it.

If you enable this policy, you can use the "Action" box to specify how computers in the group respond.

-- "Work offline" indicates that the computer can use local copies of network files while the server is inaccessible.

-- "Never go offline" indicates that network files are not available while the server is inaccessible.

If you disable this policy or select the "Work offline" option, users can work offline if disconnected.

If you do not configure this policy, users can work offline by default, but they can change this option.

This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Tip: To configure this setting without establishing a policy, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, click Advanced, and then select an option in the "When a network connection is lost" section (Microsoft Developer's Network, 2000).

### ***Non-default server disconnect actions***

Determines how computers respond when they are disconnected from particular offline file servers. This policy overrides the default response, a user-specified response, and the response specified in the "Action on server disconnect" policy.

This policy also disables the "Exception list" section on the Offline Files tab. This prevents users from trying to change the option while a policy controls it.

To use this policy, click Show, and then click Add. In the "Type the name of the item to be added" box, type the server's computer name. Then, in the "Type the value of the item to be added" box, type "0" if users can work offline when they are disconnected from this server, or type "1" if they cannot.

This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Tip: To configure this setting without establishing a policy, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then click Advanced. This policy corresponds to the settings in the "Exception list" section (Microsoft Developer's Network, 2000).

### ***Disable "Make available offline"***

Prevents users from making network files and folders available offline.

This policy removes the "Make Available Offline" option from the File menu and from all context menus in Windows Explorer. As a result, users cannot designate files to be saved on their computer for offline use.

However, this policy does not prevent the system from saving local copies of files that reside on network shares designated for automatic caching.

This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration (Microsoft Developer's Network, 2000).

### ***Prevent use of offline files folder***

Disables the Offline Files folder.

This policy disables the "View Files" button on the Offline Files tab. As a result, users cannot use the Offline Files folder to view or open copies of network files stored on their computer. Also, they cannot use the folder to view characteristics of offline files, such as their server status, type, or location.

This policy does not prevent users from working offline or from saving local copies of files available offline. Also, it does not prevent them from using other programs, such as Windows Explorer, to view their offline files.

This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Tip: To view the Offline Files Folder, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then click "View Files" (Microsoft Developer's Network, 2000).

### ***Files not cached***

Lists types of files that cannot be used offline.

This policy lets you exclude certain types of files from automatic and manual caching for offline use. The system does not cache files of the type specified in this policy even when they reside on a network share configured for automatic caching. Also, if users try to make a file of this type available offline, the operation will fail and the following message will be displayed in the Synchronization Manager progress dialog box: "Files of this type cannot be made available offline."

This policy is designed to protect files that cannot be separated, such as database components.

To use this policy, type the file name extension in the "Extensions" box. To type more than one extension, separate the extensions with a semicolon (;).

Note: To make changes to this policy effective, you must log off and log on again (Microsoft Developer's Network, 2000).

### ***Administratively assigned offline files***

Lists network files and folders that are always available for offline use. This policy makes the specified files and folders available offline to users of the computer.

To assign a folder, click Show and then click Add. In the "Type the name of the item to be added" box, type the fully qualified UNC path to the file or folder. Leave the "Enter the value of the item to be added" field blank.

Note: This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration (Microsoft Developer's Network, 2000).

### ***Disable reminder balloons***

Hides or displays reminder balloons, and prevents users from changing the setting.

Reminder balloons appear above the Offline Files icon in the status area to notify users when they have lost the connection to a networked file and are working on a local copy of the file. Users can then decide how to proceed.

If you enable this policy, the system hides the reminder balloons, and prevents users from displaying them.

If you disable the policy, the system displays the reminder balloons, and prevents users from hiding them.

If this policy is not configured, reminder balloons are displayed by default when you enable offline files, but users can change the setting.

To prevent users from changing the setting while a policy is in effect, the system disables the "Enable reminders" option on the Offline Files tab (Microsoft Developer's Network, 2000).

### ***Reminder balloon frequency***

Determines how often reminder balloon updates appear.

This policy also removes the "Display reminder balloon every ... minutes" option on the Offline Files tab. This prevents users from trying to change the option while a policy controls it.

Reminder balloons appear when the user's connection to a network file is lost or reconnected and are updated periodically. By default, the first reminder for an event is displayed for 30 seconds. Then, updates appear every 60 minutes and are displayed for 15 seconds. You can use this policy to change the update interval.

This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Tip: To set reminder balloon frequency without establishing a policy, in Windows Explorer, on the Tools menu, click Folder Options, and then click the Offline Files tab. This policy corresponds to the "Display reminder balloons every ... minutes" option (Microsoft Developer's Network, 2000).

### ***Initial reminder balloon lifetime***

Determines how long the first reminder balloon for a network status change is displayed.

Reminder balloons appear when the user's connection to a network file is lost or reconnected and are updated periodically. By default, the first reminder for an event is displayed for 30 seconds. Then, updates appear every 60 minutes and are displayed for 15 seconds. You can use this policy to change the duration of the first reminder.

This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration (Microsoft Developer's Network, 2000).

### ***Reminder balloon lifetime***

Determines how long updated reminder balloons are displayed.

Reminder balloons appear when the user's connection to a network file is lost or reconnected and are updated periodically. By default, the first reminder for an event is displayed for 30 seconds. Then, updates appear every 60 minutes and are displayed for 15 seconds. You can use this policy to change the duration of the update reminder.

This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration (Microsoft Developer's Network, 2000).

### ***At logoff, delete local copy of user's offline files***

Deletes local copies of the user's offline files when the user logs off.

This policy specifies that automatically and manually cached offline files are retained only while the user is logged on to the computer. When the user logs off, the system deletes all local copies of offline files.

If you disable this policy or do not configure it, automatically and manually cached copies are retained on the user's computer for later offline use.

Caution: Files are not synchronized before they are deleted. Any changes to local files since the last synchronization are lost (Microsoft Developer's Network, 2000).

### ***Event logging level***

Determines which events the Offline Files feature records in the event log.

Offline Files records events in the Application log in Event Viewer when it detects errors. By default, Offline Files records an event only when the offline files storage cache is corrupted. However, you can use this policy to specify additional events you want Offline Files to record.

To use this policy, from the "Enter" box, select the number corresponding to the events you want the system to log. The levels are cumulative; that is, each level includes the events in all preceding levels.

"0" records an error when the offline storage cache is corrupted.

"1" also records an event when the server hosting the offline file is disconnected from the network.

"2" also records events when the local computer is connected and disconnected from the network.

"3" also records an event when the server hosting the offline file is reconnected to the network.

Note: This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration (Microsoft Developer's Network, 2000).

### ***Subfolders always available offline***

Makes subfolders available offline whenever their parent folder is made available offline.

This policy automatically extends the "make available offline" setting to all new and existing subfolders of a folder. Users do not have the option of excluding subfolders.

If you enable this policy, then when you make a folder available offline, all folders within that folder are

also made available offline. Also, new folders that you create within a folder that is available offline are made available offline when the parent folder is synchronized.

If you disable this policy or do not configure it, the system asks users whether they want subfolders to be made available offline when they make a parent folder available offline (Microsoft Developer's Network, 2000).

### ***Network and Dial-up Connections***

#### ***Allow configuration of connection sharing***

Determines whether administrators can enable, disable, and configure the Internet Connection Sharing feature of a dial-up connection.

If you enable this policy or do not configure it, the system displays the Internet Connection Sharing (ICS) tab in the Properties dialog box for a dial-up connection. On Windows 2000 Server, it also displays the Internet Connection Sharing page in the Network Connection wizard. (This page is available only in Windows 2000 Server.)

If you disable this policy, the Internet Connection Sharing (ICS) tab and Internet Connection Sharing wizard page are removed.

Internet Connection Sharing lets users configure their system as an Internet gateway for a small network. It provides network services, such as name resolution, to the network.

By default, Internet Connection Sharing is disabled when you create a dial-up connection, but administrators can use the Internet Connection Sharing (ICS) tab and Internet Connection Sharing wizard page to enable it.

Note: This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Important: This policy applies only to users in the Administrators group (Microsoft Developer's Network, 2000).

### **Printers**

#### ***Allow printers to be published***

Determines whether the computer's shared printers can be published in Active Directory.

If you enable this policy or do not configure it, users can use the "List in directory" option in the Printers folder or the Add Printer wizard to publish shared printers in Active Directory.

If you disable this policy, this computer's shared printers cannot be published in Active Directory and the "List in directory" option is disabled (Microsoft Developer's Network, 2000).

### ***Automatically new printers in active directory***

Determines whether the Add Printer wizard automatically publishes the computer's shared printers in Active Directory.

If you enable this policy or do not configure it, the Add Printer wizard automatically publishes all shared printers.

If you disable this policy, the Add Printer wizard does not automatically publish printers. However, you can publish shared printers manually.

Note: This policy is ignored if the "Allow printers to be published" policy is disabled (Microsoft Developer's Network, 2000).

### ***Allow pruning of published printers***

Determines whether the domain controller can prune (delete from Active Directory) the printers published by this computer.

By default, the pruning service on the domain controller prunes printer objects from Active Directory if the computer that published them does not respond to contact requests. When the computer that published the printers restarts, it republishes any deleted printer objects.

If you enable this policy or do not configure it, the domain controller prunes this computer's printers when the computer does not respond.

If you disable this policy, the domain controller does not prune this computer's printers. This setting is designed to prevent printers from being pruned when the computer is temporarily disconnected from the network.

Note: You can use the "Directory Pruning Interval" and "Directory Pruning Retry" policies to adjust the contact interval and number of contact attempts (Microsoft Developer's Network, 2000).

### ***Printer browsing***

Announces the presence of shared printers to print browse master servers for the domain.

On Windows 2000 domains with Active Directory, shared printer resources are available in Active Directory and are not announced.

If you enable this policy, the print spooler announces shared printers to the print browse master servers. As a result, shared printers appear in the domain list in the Browse for Printer dialog box of the Add Printer wizard.



If you disable this policy, shared printers are not announced to print browse master servers, even if Active Directory is not available.

If you do not configure this policy, shared printers are announced to browse master servers only when Active Directory is not available.

Note: A client license is used each time a client computer announces a printer to a print browse master on the domain (Microsoft Developer's Network, 2000).

### ***Prune printers that are not automatically republished***

Determines whether the system prunes (deletes from Active Directory) printers that are not automatically republished. This policy applies to printers running operating systems other than Windows 2000 and to Windows 2000 printers published outside of their domain.

The Windows 2000 pruning service prunes printer objects from Active Directory when the computer that published them does not respond to contact requests. Computers running Windows 2000 detect and republish deleted printer objects when they rejoin the network. However, because non-Windows 2000 computers and computers in other domains cannot republish printers in Active Directory automatically, then, by default, the system never prunes their printer objects.

You can enable this policy to change the default behavior. To use this policy, select one of the following options from the "Prune non-republishing printers" box:

- "Never" specifies that printer objects that are not automatically republished are never pruned. "Never" is the default.
- "Only if Print Server is found" prunes printer objects that are not automatically republished only when the print server responds, but the printer is unavailable.
- "Whenever printer is not found" prunes printer objects that are not automatically republished whenever the host computer does not respond, just as it does with Windows 2000 printers.

Note: This policy applies to printers published by using Active Directory Users and Computers or Pubprn.vbs. It does not apply to printers published by using Printers in Control Panel.

Tip: If you disable automatic pruning, remember to delete printer objects manually whenever you remove a printer or print server (Microsoft Developer's Network, 2000).

### ***Directory pruning interval***

Specifies how often the pruning service on a domain controller contacts computers to verify that their printers are operational.

The pruning service periodically contacts computers that have published printers. If a computer does not respond to the contact message (optionally, after repeated attempts), the pruning service "prunes" (deletes from Active Directory) printer objects the computer has published.

By default, the pruning service contacts computers every eight hours and allows two repeated contact attempts before deleting printers from Active Directory. You can use this policy to change the interval between contact attempts. To change the number of attempts, use the "Directory Pruning Retry" policy.

Note: This policy is used only on domain controllers (Microsoft Developer's Network, 2000).

### ***Directory pruning retry***

Specifies how many times the pruning service on a domain controller repeats its attempt to contact a computer before pruning the computer's printers.

The pruning service periodically contacts computers that have published printers to verify that the printers are still available for use. If a computer does not respond to the contact message, the message is repeated for the specified number of times. If the computer still fails to respond, then the pruning service "prunes" (deletes from Active Directory) printer objects the computer has published.

By default, the pruning service contacts computers every eight hours and allows two retries before deleting printers from Active Directory. You can use this policy to change the number of retries. To change the interval between attempts, use the "Directory Pruning Interval" policy.

Note: This policy is used only on domain controllers (Microsoft Developer's Network, 2000).

### ***Directory pruning priority***

Sets the priority of the pruning thread.

The pruning thread, which runs only on domain controllers, deletes printer objects from Active Directory if the printer that published the object does not respond to contact attempts. This process keeps printer information in Active Directory current.

The thread priority influences the order in which the thread receives processor time and determines how likely it is to be preempted by higher priority threads.

By default, the pruning thread runs at normal priority. However, you can adjust the priority to improve the performance of this service.

Note: This policy is used only on domain controllers (Microsoft Developer's Network, 2000).

### ***Check published state***

Directs the system to periodically verify that the printers published by this computer still appear in Active Directory. Also, this policy specifies how often the system repeats the verification.

By default, the system verifies published printers when it starts. This policy provides for periodic verification while the computer is operating.

To enable this additional verification, enable this policy, and then select a verification interval.

To disable verification, disable or do not configure this policy, or set the verification interval to "Never (Microsoft Developer's Network, 2000).

### ***Web based printing***

Determines whether Internet printing is supported on this server.

Internet printing lets you display printers on Web pages so the printers can be viewed, managed, and used across the Internet or an intranet.

Internet printing is supported by default on Windows 2000. If you enable this policy or do not configure it, Internet printing remains supported. If you disable this policy, Internet printing is not supported.

Note: This policy affects the server side of Internet printing only. It does not prevent the print client on the computer from printing across the Internet (Microsoft Developer's Network, 2000).

### ***Custom support URL in the printer's folders left pane***

Adds a customized Web page link to the Printers folder.

By default, the Printers folder includes a link to the Microsoft Support Web page. It can also include a link to a Web page supplied by the vendor of the currently selected printer.

You can use this policy to replace these default links with a link to a Web page customized for your enterprise.

If you disable this policy, do not configure it or if you do not enter an alternate Internet address, the default links appear in the Printers folder.

Note: Web pages links only appear in the Printers folder when Web view is enabled. If Web view is disabled, the policy has no effect. (To enable Web view, open the Printers folder, and from the Tools menu, click Folder Options, click the General tab, and then click "Enable Web content in folders.")

Also, see the "Web-based printing" policy in this policy folder and the "Browse a common web site to find printers" policy in User Configuration\Administrative Templates\Control Panel\Printers.

Web view is affected by the "Enable Classic Shell" and "Remove the Folder Options menu item from the Tools menu" policies in User Configuration\Administrative Templates\Windows Components\Windows Explorer, and by the "Enable Active Desktop" policy in User Configuration\Administrative Templates\Desktop\Active Desktop (Microsoft Developer's Network, 2000).

### ***Computer location***

Specifies the default location criteria used when searching for printers.

This policy is a component of the Location Tracking feature of Windows 2000 printers. To use this policy, enable Location Tracking by enabling the "Pre-populate printer search location text" policy.

When Location Tracking is enabled, the system uses the specified location as a criteria when users search for printers. The value you type here overrides the actual location of the computer conducting the search.

Type the location of the user's computer. When users search for printers, the system uses the specified location (and other search criteria) to find a printer nearby. You can also use this policy to direct users to a particular printer or group of printers that you want them to use.

If you disable this policy or do not configure it and the user does not type a location as a search criteria, the system searches for a nearby printer based on the IP address and subnet mask of the user's computer (Microsoft Developer's Network, 2000).

### ***Pre-populate printer search location text***

Enables the physical Location Tracking support feature of Windows 2000 printers.

Location tracking lets you design a location scheme for your enterprise and assign computers and printers to locations in your scheme. Location tracking overrides the standard method of locating and associating users and printers, which uses the IP address and subnet mask of a computer to estimate its physical location and proximity to other computers.

If you enable Location Tracking, a Browse button appears beside the Location field in the Find Printers dialog box. (To go to the Browse button, click Start, click Search, and click For printers.) The Browse button also appears on the General tab of the Properties dialog box for a printer. It lets users browse for printers by location without their having to know the precise location (or location naming scheme). Also, if you enable the "Computer location" policy, the default location you type appears in the Location field.

If you disable this policy or do not configure it, Location Tracking is disabled. Printer proximity is estimated based on IP address and subnet mask (Microsoft Developer's Network, 2000).

## USER CONFIGURATION

### SOFTWARE SETTINGS

#### Software installation

### WINDOWS SETTINGS

#### IE maintenance

##### *Browser user interface*

- (9) Browser Title
- (10) Animated Bitmaps
- (11) Custom Logo
- (12) Browser Toolbar buttons

##### *Connection*

- (13) Connection Settings
- (14) Automated Browser configuration
- (15) Proxy settings
- (16) User agent strings

##### *URLs*

- (17) Favorites and Links
- (18) Important URLs
- (19) Channels

##### *Security*

- (20) Security Zones and content ratings
- (21) Authenticode settings

##### *Programs*

- (22) Programs

#### Scripts

##### *Logon*

##### *Logoff*

## Security Settings

### *Public key policies*

(23) Enterprise trust

### *Remote Installation Service*

(24) Choice options

## Folder Redirection

### *Application Data*

### *Desktop*

### *My Documents*

(25) My Pictures

### *Start Menu*

## ADMINISTRATIVE TEMPLATES

## Windows Components

### *Netmeeting*

#### ***Enable automatic configuration***

Configures NetMeeting to download settings for users each time it starts.

The settings are downloaded from the URL listed in the "Configuration URL:" text box.

Group Policy based settings have precedence over any conflicting settings set by downloading them from this URL (Microsoft Developer's Network, 2000).

#### ***Disable directory services***

Disables the directory feature of NetMeeting.

Users will not logon to a directory (ILS) server when NetMeeting starts. Users will also not be able to view or place calls via a NetMeeting directory.

This policy is for deployers who have their own location or calling schemes such as a Web site or an address book (Microsoft Developer's Network, 2000).

#### ***Prevent adding directory servers***

Prevents users from adding directory (ILS) servers to the list of those they can use for placing calls (Microsoft Developer's Network, 2000).

#### ***Prevent viewing web directory***

Prevents users from viewing directories as Web pages in a browser (Microsoft Developer's Network, 2000).

#### ***Set the intranet support page***

Sets the URL NetMeeting will display when the user chooses the Help Online Support command.

#### ***Set call security option***

Sets the level of security for both outgoing and incoming NetMeeting calls (Microsoft Developer's Network, 2000).

***Prevent changing call placement method***

Prevents users from changing the way calls are placed, either directly or via a gatekeeper server (Microsoft Developer's Network, 2000).

***Prevent automatic acceptance of calls***

Prevents users from turning on automatic acceptance of incoming calls.

This ensures that others cannot call and connect to NetMeeting when the user is not present.

This policy is recommended when deploying NetMeeting to run always (Microsoft Developer's Network, 2000).

***Prevent sending files***

Prevents users from sending files to others in a conference (Microsoft Developer's Network, 2000).

***Prevent receiving files***

Prevents users from receiving files from others in a conference (Microsoft Developer's Network, 2000).

***Limit the size of sent files***

Limits the size of files users can send to others in a conference (Microsoft Developer's Network, 2000).

***Disable chat***

Disables the Chat feature of NetMeeting (Microsoft Developer's Network, 2000).

***Disable Netmeeting 2.X whiteboard***

Disables the 2.x whiteboard feature of NetMeeting.

The 2.x whiteboard is available for compatibility with older versions of NetMeeting only.

Deployers who do not need it can save bandwidth by disabling it (Microsoft Developer's Network, 2000).

***Disable whiteboard***

Disables the T.126 whiteboard feature of NetMeeting (Microsoft Developer's Network, 2000).

(26) Application Sharing

**(i) *Disable Application sharing***

**(ii)** Disables the application-sharing feature of NetMeeting completely. Users will



not be able to host or view shared applications (Microsoft Developer's Network, 2000).

***Prevent sharing***

Prevents users from sharing anything themselves. They will still be able to view shared applications/desktops from others (Microsoft Developer's Network, 2000).

***Prevent desktop sharing***

Prevents users from sharing the whole desktop. They will still be able to share individual applications (Microsoft Developer's Network, 2000).

***Prevent sharing command prompts***

Prevents users from sharing command prompts. This prevents users from inadvertently sharing out applications, since command prompts can be used to launch other applications (Microsoft Developer's Network, 2000).

***Prevent sharing explorer windows***

Prevents users from sharing Explorer windows. This prevents users from inadvertently sharing out applications, since Explorer windows can be used to launch other applications (Microsoft Developer's Network, 2000).

***Prevent control***

Prevents users from allowing others in a conference to control what they have shared. This enforces a read-only mode; the other participants cannot change the data in the shared application (Microsoft Developer's Network, 2000).

***Prevent application sharing in true color***

Prevents users from sharing applications in true color. True color sharing uses more bandwidth in a conference (Microsoft Developer's Network, 2000).

(27) Audio and Video

***(i) Limit the bandwidth of audio and video***

***(ii)*** Limits the bandwidth audio and video will consume when in a conference. This

setting will guide NetMeeting to choose the right formats and send rate so that the bandwidth is limited (Microsoft Developer's Network, 2000).

***Disable audio***

Disables the audio feature of NetMeeting. Users will not be able to send or receive audio (Microsoft Developer's Network, 2000).

***Disable full duplex audio***

Disables full duplex mode audio. Users will not be able to listen to incoming audio while speaking into the microphone. Older audio hardware does not perform well when in full duplex mode (Microsoft Developer's Network, 2000).

***Prevent changing direct sound audio settings***

Prevents user from changing the DirectSound audio setting. DirectSound provides much better audio quality, but older audio hardware may not support it (Microsoft Developer's Network, 2000).

***Prevent sending video***

Prevents users from sending video if they have the hardware. Users will still be able to receive video from others (Microsoft Developer's Network, 2000).

***Prevent receiving video***

Prevents users from receiving video. Users will still be able to send video provided they have the hardware (Microsoft Developer's Network, 2000).

(28) Options Page

***Hide the general page***

Hides the General page of the Tools Options dialog. Users will not then be able to change personal identification and bandwidth settings (Microsoft Developer's Network, 2000).

***Disable the advanced calling button***

Disables the Advanced Calling button on the General Options page. Users will not then be able to change the call placement method and the servers used (Microsoft Developer's Network, 2000).

***Hide the security page***

Hides the Security page of the Tools Options dialog. Users will not then be able to change call security and authentication settings (Microsoft Developer's Network, 2000).

***Hide the audio page***

Hides the Audio page of the Tools Options dialog. Users will not then be able to change audio settings (Microsoft Developer's Network, 2000).

***Hide the video page***

Hides the Video page of the Tools Options dialog. Users will not then be able to change video settings (Microsoft Developer's Network, 2000).

***Internet Explorer***

***Search: Disable search customization***

Makes the Customize button in the Search Assistant appear dimmed.

The Search Assistant is a tool that appears in the Search bar to help users search the Internet.

If you enable this policy, users cannot change their Search Assistant settings, such as setting default search engines for specific tasks.

If you disable this policy or do not configure it, users can change their settings for the Search Assistant.

This policy is designed to help administrators maintain consistent settings for searching across an organization (Microsoft Developer's Network, 2000).

***Search: Disable find files via F3 within browser***

Disables using the F3 key to search in Internet Explorer and Windows Explorer.

If you enable this policy, the search functionality of the F3 key is disabled. Users cannot press F3 to search the Internet (from Internet Explorer) or to search the hard disk (from Windows Explorer). If the user presses F3, a prompt appears that informs the user that this feature has been disabled.

If you disable this policy or do not configure it, users can press F3 to search the Internet (from Internet Explorer) or the hard disk (from Windows Explorer).

This policy is intended for situations in which administrators do not want users to explore the Internet or the hard disk.

This policy can be used in coordination with the "File Menu: Disable Open menu option" policy (located in \User Configuration\Administrative Templates\Windows

Components\Internet Explorer\Browser Menus), which prevents users from opening files by using the browser (Microsoft Developer's Network, 2000).

### ***Disable external branding of IE***

Prevents branding of Internet programs, such as customization of Internet Explorer and Outlook Express logos and title bars, by a third party.

If you enable this policy, it prevents customization of the browser by a third party, such as an Internet service provider or Internet content provider.

If you disable this policy or do not configure it, users could install customizations from a third party—for example, when signing up for Internet services.

This policy is intended for administrators who want to maintain a consistent browser across an organization (Microsoft Developer's Network, 2000).

### ***Disable importing and exporting of favorites***

Prevents users from exporting or importing favorite links by using the Import/Export wizard.

If you enable this policy, the Import/Export wizard cannot import or export favorite links or cookies, which are small text files that contain settings for Web sites.

If you disable this policy or do not configure it, users can import and export favorites in Internet Explorer by clicking the File menu, clicking Import and Export, and then running the Import/Export wizard.

Note: If you enable this policy, users can still view screens in the wizard, but when users click Finish, a prompt will appear that states that this feature has been disabled (Microsoft Developer's Network, 2000).

### ***Disable changing advanced page settings***

Prevents users from changing settings on the Advanced tab in the Internet Options dialog box.

If you enable this policy, users are prevented from changing advanced Internet settings, such as security, multimedia, and printing. Users cannot select or clear the check boxes on the Advanced tab.

If you disable this policy or do not configure it, users can select or clear settings on the Advanced tab.

If you set the "Disable the Advanced page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the "Disable the Advanced page" policy

removes the Advanced tab from the interface (Microsoft Developer's Network, 2000).

### ***Disable changing home page settings***

Prevents users from changing the home page of the browser. The home page is the first page that appears when users start the browser.

If you enable this policy, the settings in the Home Page area on the General tab in the Internet Options dialog box appear dimmed.

If you disable this policy or do not configure it, users can change their home page.

If you set the "Disable the General page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the "Disable the General page" policy removes the General tab from the interface.

This policy is intended for administrators who want to maintain a consistent home page across their organization (Microsoft Developer's Network, 2000).

### ***Use automatic detection for dial-up connections***

Specifies that Automatic Detection will be used to configure dial-up settings for users.

Automatic Detection uses a DHCP (Dynamic Host Configuration Protocol) or DNS (Domain Name System) server to customize the browser the first time it is started.

If you enable this policy, the users' dial-up settings will be configured by Automatic Detection.

If you disable this policy or do not configure it, the dial-up settings will not be configured by Automatic Detection, unless specified by the user (Microsoft Developer's Network, 2000).

### ***Disable caching of auto-proxy scripts***

Prevents automatic proxy scripts, which interact with a server to automatically configure users' proxy settings, from being stored in the users' cache.

If you enable this policy, automatic proxy scripts will not be stored temporarily on the users' computer.

If you disable this policy or do not configure it, automatic proxy scripts can be stored in the users' cache (Microsoft Developer's Network, 2000).

### ***Display error message on proxy script download failure***

Specifies that error messages will be displayed to users if problems occur with proxy scripts.

If you enable this policy, error messages will be displayed when the browser does not download or run a script to set proxy settings.

If you disable this policy or do not configure it, error messages will not be displayed when problems occur with proxy scripts (Microsoft Developer's Network, 2000).

### ***Disable changing temporary internet files settings***

Prevents users from changing the browser cache settings, such as the location and amount of disk space to use for the Temporary Internet Files folder.

If you enable this policy, the browser cache settings appear dimmed. These settings are found in the dialog box that appears when users click the General tab and then click the Settings button in the Internet Options dialog box.

If you disable this policy or do not configure it, users can change their cache settings.

If you set the "Disable the General page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the "Disable the General page" policy removes the General tab from the interface (Microsoft Developer's Network, 2000).

### ***Disable changing history settings***

Prevents users from changing the history settings for the browser.

If you enable this policy, the settings in the History area on the General tab in the Internet Options dialog box appear dimmed.

If you disable this policy or do not configure it, users can change the number of days to store Web page information and clear Web page history.

If you set the "Disable the General page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the "Disable the General page" policy removes the General tab from the interface (Microsoft Developer's Network, 2000).

### ***Disable changing color settings***

Prevents users from changing the default Web page colors.

If you enable this policy, the color settings for Web pages appear dimmed. The settings are located in the Colors area in the dialog box that appears when the user clicks the General tab and then clicks the Colors button in the Internet Options dialog box.

If you disable this policy or do not configure it, users can change the default background and text color of Web pages.

If you set the "Disable the General page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the "Disable the General page" policy removes the General tab from the interface.

Note: The default Web page colors are ignored on Web pages in which the author has specified the background and text colors (Microsoft Developer's Network, 2000).

### ***Disable changing link color settings***

Prevents users from changing the colors of links on Web pages.

If you enable this policy, the color settings for links appear dimmed. The settings are located in the Links area of the dialog box that appears when users click the General tab and then click the Colors button in the Internet Options dialog box.

If you disable this policy or do not configure it, users can change the default color of links on Web pages.

If you set the "Disable the General page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the "Disable the General page" policy removes the General tab from the interface.

Note: The default link colors are ignored on Web pages on which the author has specified link colors (Microsoft Developer's Network, 2000).

### ***Disable changing font settings***

Prevents users from changing font settings.

If you enable this policy, the Font button on the General tab in the Internet Options dialog box appears dimmed.

If you disable this policy or do not configure it, users can change the default fonts for viewing Web pages.

If you set the "Disable the General page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the "Disable the General page" policy removes the General tab from the interface.

Note: The default font settings colors are ignored in cases in which the Web page author has specified the font attributes (Microsoft Developer's Network, 2000).

### ***Disable changing language settings***

Prevents users from changing language settings.

If you enable this policy, the Languages button on the General tab in the Internet Options dialog box appears dimmed.

If you disable this policy or do not configure it, users can change the language settings for viewing Web sites for languages in which the character set has been installed.

If you set the "Disable the General page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the "Disable the General page" policy removes the General tab from the interface (Microsoft Developer's Network, 2000).

### ***Disable changing accessibility settings***

Prevents users from changing accessibility settings.

If you enable this policy, the Accessibility button on the General tab in the Internet Options dialog box appears dimmed.

If you disable this policy or do not configure it, users can change accessibility settings, such as overriding fonts and colors on Web pages.

If you set the "Disable the General page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the "Disable the General page" policy removes the General tab from the interface (Microsoft Developer's Network, 2000).

### ***Disable internet connection wizard***

Prevents users from running the Internet Connection wizard.



If you enable this policy, the Setup button on the Connections tab in the Internet Options dialog box appears dimmed.

Users will also be prevented from running the wizard by clicking the Connect to the Internet icon on the desktop or by clicking Start, pointing to Programs, pointing to Accessories, pointing to Communications, and then clicking Internet Connection wizard.

If you disable this policy or do not configure it, users can change their connection settings by running the Internet Connection wizard.

Note: This policy overlaps with the "Disable the Connections page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Connections tab from the interface. Removing the Connections tab from the interface, however, does not prevent users from running the Internet Connection wizard from the desktop or the Start menu (Microsoft Developer's Network, 2000).

### ***Disable changing connection settings***

Prevents users from changing dial-up settings.

If you enable this policy, the Settings button on the Connections tab in the Internet Options dialog box appears dimmed.

If you disable this policy or do not configure it, users can change their settings for dial-up connections.

If you set the "Disable the Connections page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), you do not need to set this policy, because the "Disable the Connections page" policy removes the Connections tab from the interface (Microsoft Developer's Network, 2000).

### ***Disable changing proxy settings***

Prevents users from changing proxy settings.

If you enable this policy, the proxy settings appear dimmed. These settings are in the Proxy Server area of the Local Area Network (LAN) Settings dialog box, which appears when the user clicks the Connections tab and then clicks the LAN Settings button in the Internet Options dialog box.

If you set the "Disable the Connections page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet

Explorer\Internet Control Panel), you do not need to set this policy, because the "Disable the Connections page" policy removes the Connections tab from the interface (Microsoft Developer's Network, 2000).

### ***Disable changing automatic configuration settings***

Prevents users from changing automatic configuration settings. Automatic configuration is a process that administrators can use to update browser settings periodically.

If you enable this policy, the automatic configuration settings appear dimmed. The settings are located in the Automatic Configuration area of the Local Area Network (LAN) Settings dialog box. To see the Local Area Network (LAN) Settings dialog box, users open the Internet Options dialog box, click the Connections tab, and then click the LAN Settings button.

If you disable this policy or do not configure it, the user can change automatic configuration settings.

This policy is intended to enable administrators to ensure that users' settings are updated uniformly through automatic configuration.

The "Disable the Connections page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Connections tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored (Microsoft Developer's Network, 2000).

### ***Disable changing ratings settings***

Prevents users from changing ratings that help control the type of Internet content that can be viewed.

If you enable this policy, the settings in the Content Advisor area on the Content tab in the Internet Options dialog box appear dimmed.

If you disable this policy or do not configure it, users can change their ratings settings.

The "Disable the Ratings page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Ratings tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored (Microsoft Developer's Network, 2000).

### ***Disable changing certificate settings***

Prevents users from changing certificate settings in Internet Explorer. Certificates are used to verify the identity of software publishers.

If you enable this policy, the settings in the Certificates area on the Content tab in the Internet Options dialog box appear dimmed.

If you disable this policy or do not configure it, users can import new certificates, remove approved publishers, and change settings for certificates that have already been accepted.

The "Disable the Content page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Content tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored.

Caution: If you enable this policy, users can still run the Certificate Manager Import wizard by double-clicking a software publishing certificate (.spc) file. This wizard enables users to import and configure settings for certificates from software publishers that haven't already been configured for Internet Explorer (Microsoft Developer's Network, 2000).

### ***Disable changing profile assistant settings***

Prevents users from changing Profile Assistant settings.

If you enable this policy, the My Profile button appears dimmed in the Personal Information area on the Content tab in the Internet Options dialog box.

If you disable this policy or do not configure it, users can change their profile information, such as their street and e-mail addresses.

The "Disable the Connections page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Connections tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored (Microsoft Developer's Network, 2000).

### ***Disable autocomplete for forms***

Prevents Internet Explorer from automatically completing forms, such as filling in a name or a password that the user has entered previously on a Web page.

If you enable this policy, the Forms check box appears dimmed. To display the Forms check box, users

open the Internet Options dialog box, click the Content tab, and then click the AutoComplete button.

If you disable this policy or do not configure it, users can enable the automatic completion of forms.

The "Disable the Content page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Content tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored.

Caution: If you enable this policy after users have used their browser with form automatic completion enabled, it will not clear the automatic completion history for forms that users have already filled out (Microsoft Developer's Network, 2000).

### ***Do not allow autocomplete to save passwords***

Disables automatic completion of user names and passwords in forms on Web pages, and prevents users from being prompted to save passwords.

If you enable this policy, the User Names and Passwords on Forms and Prompt Me to Save Passwords check boxes appear dimmed. To display these check boxes, users open the Internet Options dialog box, click the Content tab, and then click the AutoComplete button.

If you disable this policy or don't configure it, users can determine whether Internet Explorer automatically completes user names and passwords on forms and prompts them to save passwords.

The "Disable the Content page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Content tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored (Microsoft Developer's Network, 2000).

### ***Disable changing messaging settings***

Prevents users from changing the default programs for messaging tasks.

If you enable this policy, the E-mail, Newsgroups, and Internet Call options in the Internet Programs area appear dimmed. To display these options, users open the Internet Options dialog box, and then click the Programs tab.

If you disable this policy or do not configure it, users can determine which programs to use for sending mail, viewing newsgroups, and placing Internet calls, if programs that perform these tasks are installed.

The "Disable the Programs page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Programs tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored (Microsoft Developer's Network, 2000).

### ***Disable changing calendar and contact settings***

Prevents users from changing the default programs for managing schedules and contacts.

If you enable this policy, the Calendar and Contact check boxes appear dimmed in the Internet Programs area. To display these options, users open the Internet Options dialog box, and then click the Programs tab.

If you disable this policy or do not configure it, users can determine which programs to use for managing schedules and contacts, if programs that perform these tasks are installed.

This "Disable the Programs Page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel) takes precedence over this policy. If it is enabled, this policy is ignored (Microsoft Developer's Network, 2000).

### ***Disable the reset web settings feature***

Prevents users from restoring default settings for home and search pages.

If you enable this policy, the Reset Web Settings button on the Programs tab in the Internet Options dialog box appears dimmed.

If you disable this policy or do not configure it, users can restore the default settings for home and search pages.

The "Disable the Programs page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Programs tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored (Microsoft Developer's Network, 2000).

### ***Disable changing default browser check***

Prevents Internet Explorer from checking to see whether it is the default browser.

If you enable this policy, the Internet Explorer Should Check to See Whether It Is the Default Browser check box on the Programs tab in the Internet Options dialog box appears dimmed.

If you disable this policy or do not configure it, users can determine whether Internet Explorer will check to see if it is the default browser. When Internet Explorer performs this check, it prompts the user to specify which browser to use as the default.

This policy is intended for organizations that do not want users to determine which browser should be their default.

The "Disable the Programs page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Programs tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored (Microsoft Developer's Network, 2000).

### ***Identity manager: Prevent users from using Identities***

Prevents users from configuring unique identities by using Identity Manager.

Identity Manager enables users to create multiple accounts, such as e-mail accounts, on the same computer. Each user has a unique identity, with a different password and different program preferences.

If you enable this policy, users will not be able to create new identities, manage existing identities, or switch identities. The Switch Identity option will be removed from the File menu in Address Book.

If you disable this policy or do not configure it, users can set up and change identities (Microsoft Developer's Network, 2000).

(29) Internet Control Panel

### ***Disable the general page***

Removes the General tab from the interface in the Internet Options dialog box.

If you enable this policy, users are unable to see and change settings for the home page, the cache, history, Web page appearance, and accessibility.

If you disable this policy or do not configure it, users can see and change these settings.

When you set this policy, you do not need to set the following Internet Explorer policies (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\), because this policy removes the General tab from the interface:

- "Disable changing home page settings"

- "Disable changing Temporary Internet files settings"

- "Disable changing history settings"

- "Disable changing color settings"

- "Disable changing link color settings"

- "Disable changing font settings"

- "Disable changing language settings"

- "Disable changing accessibility settings"

(Microsoft Developer's Network, 2000).

### ***Disable the security page***

Removes the Security tab from the interface in the Internet Options dialog box.

If you enable this policy, it prevents users from seeing and changing settings for security zones, such as scripting, downloads, and user authentication.

If you disable this policy or do not configure it, users can see and change these settings.

When you set this policy, you do not need to set the following Internet Explorer policies, because this policy removes the Security tab from the interface:

- "Security zones: Do not allow users to change policies"

- "Security zones: Do not allow users to add/delete sites"

- "Only allow controls from Trusted Publishers"

### ***Disable the content page***

Removes the Content tab from the interface in the Internet Options dialog box.

If you enable this policy, users are prevented from seeing and changing ratings, certificates, AutoComplete, Wallet, and Profile Assistant settings.

If you disable this policy or do not configure it, users can see and change these settings.

When you set this policy, you do not need to set the following policies for the Content tab, because this policy removes the Content tab from the interface:

- "Disable changing ratings settings"

- "Disable changing certificate settings"

- "Disable changing Profile Assistant settings"

- "Disable AutoComplete for forms"

- "Do not allow AutoComplete to save passwords"

(Microsoft Developer's Network, 2000).

### ***Disable the connections page***

Removes the Connections tab from the interface in the Internet Options dialog box.

If you enable this policy, users are prevented from seeing and changing connection and proxy settings.

If you disable this policy or do not configure it, users can see and change these settings.

When you set this policy, you do not need to set the following policies for the Content tab, because this policy removes the Connections tab from the interface:

- "Disable Internet Connection Wizard"

- "Disable changing connection settings"

- "Disable changing proxy settings"

- "Disable changing Automatic Configuration settings"

(Microsoft Developer's Network, 2000).

### ***Disable the programs page***

Removes the Programs tab from the interface in the Internet Options dialog box.

If you enable this policy, users are prevented from seeing and changing default settings for Internet programs.

If you disable this policy or do not configure it, users can see and change these settings.

When you set this policy, you do not need to set the following policies for the Programs tab, because this policy removes the Programs tab from the interface:

- "Disable changing Messaging settings"



"Disable changing Calendar and Contact settings"

"Disable the Reset Web Settings feature"

"Disable changing default browser check"

(Microsoft Developer's Network, 2000).

**(i) *Disable the advanced page***

(ii) Removes the Advanced tab from the interface in the Internet Options dialog box.

(iii) If you enable this policy, users are prevented from seeing and changing advanced Internet settings, such as security, multimedia, and printing.

(iv) If you disable this policy or do not configure it, users can see and change these settings.

**(v)** When you set this policy, you do not need to set the "Disable changing Advanced page settings" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\), because this policy removes the Advanced tab from the interface (Microsoft Developer's Network, 2000).

(30) Offline Pages

***Disable adding channels***

Prevents users from adding channels to Internet Explorer.

Channels are Web sites that are updated automatically on your computer according to a schedule specified by the channel provider.

If you enable this policy, the Add Active Channel button, which appears on a channel that users haven't yet subscribed to, will be disabled. Users also cannot add content that is based on a channel, such as some of the Active Desktop items from Microsoft's Active Desktop Gallery, to their desktop.

If you disable this policy or do not configure it, users can add channels to the Channel bar or to their desktop.

Note: Most channel providers use the words Add Active Channel for this option; however, a few use different words, such as Subscribe (Microsoft Developer's Network, 2000).

### ***Disable removing channels***

Prevents users from disabling channel synchronization in Internet Explorer.

Channels are Web sites that are automatically updated on your computer according to a schedule specified by the channel provider.

If you enable this policy, users cannot prevent channels from being synchronized.

If you disable this policy or do not configure it, users can disable the synchronization of channels.

This policy is intended to help administrators ensure that users' computers are being updated uniformly across their organization.

Note: This policy does not prevent users from removing active content from the desktop interface (Microsoft Developer's Network, 2000).

### ***Disable adding schedules for offline pages***

Prevents users from specifying that Web pages can be downloaded for viewing offline. When users make Web pages available for offline viewing, they can view the content when their computer is not connected to the Internet.

If you enable this policy, users cannot add new schedules for downloading offline content. The Make Available Offline check box will be dimmed in the Add Favorite dialog box.

If you disable this policy or do not configure it, users can add new offline content schedules.

This policy is intended for organizations that are concerned about server load for downloading content.

The "Hide Favorites menu" policy (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer) takes precedence over this policy. If it is

enabled, this policy is ignored (Microsoft Developer's Network, 2000).

### ***Disable editing schedules for offline pages***

Prevents users from editing an existing schedule for downloading Web pages for offline viewing.

When users make Web pages available for offline viewing, they can view content when their computer is not connected to the Internet.

If you enable this policy, users cannot display the schedule properties of pages that have been set up for offline viewing. If users click the Tools menu, click Synchronize, select a Web page, and then click the Properties button, no properties are displayed. Users do not receive an alert stating that the command is unavailable.

If you disable this policy or do not configure it, users can edit an existing schedule for downloading Web content for offline viewing.

This policy is intended for organizations that are concerned about server load for downloading content.

The "Hide Favorites menu" policy (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer) takes precedence over this policy. If it is enabled, this policy is ignored (Microsoft Developer's Network, 2000).

### ***Disable removing schedules for offline pages***

Prevents users from clearing the preconfigured settings for Web pages to be downloaded for offline viewing.

When users make Web pages available for offline viewing, they can view content when their computer is not connected to the Internet.

If you enable this policy, the Make Available Offline check box in the Organize Favorites Favorite dialog box and the Make This Page Available Offline check box will be selected but dimmed. To display the Make This Page Available Offline check box, users click the Tools menu, click Synchronize, and then click the Properties button.

If you disable this policy or do not configure it, users can remove the preconfigured settings for pages to be downloaded for offline viewing.

This policy is intended for organizations that are concerned about server load for downloading content.

The "Hide Favorites menu" policy (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer) takes precedence over this policy. If it is enabled, this policy is ignored (Microsoft Developer's Network, 2000).

### ***Disable offline pages hit logging***

Prevents channel providers from recording information about when their channel pages are viewed by users who are working offline.

If you enable this policy, it disables any channel logging settings set by channel providers in the channel definition format (.cdf) file. The .cdf file determines the schedule and other settings for downloading Web content.

If you disable this policy or do not configure it, channel providers can record information about when their channel pages are viewed by users who are working offline (Microsoft Developer's Network, 2000).

### ***Disable all scheduled offline pages***

Disables existing schedules for downloading Web pages for offline viewing.

When users make Web pages available for offline viewing, they can view content when their computer is not connected to the Internet.

If you enable this policy, the check boxes for schedules on the Schedule tab of the Web page properties are cleared and users cannot select them. To display this tab, users click the Tools menu, click Synchronize, select a Web page, click the Properties button, and then click the Schedule tab.

If you disable this policy, then Web pages can be updated on the schedules specified on the Schedule tab.

This policy is intended for organizations that are concerned about server load for downloading content.

The "Hide Favorites menu" policy (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer) takes precedence over this policy. If it is enabled, this policy is ignored (Microsoft Developer's Network, 2000).

### ***Disable channel user interface completely***

Prevents users from viewing the Channel bar interface. Channels are Web sites that are automatically updated on their computer according to a schedule specified by the channel provider.

If you enable this policy, the Channel bar interface will be disabled, and users cannot select the Internet Explorer Channel Bar check box on the Web tab in the Display Properties dialog box.

If you disable this policy or do not configure it, users can view and subscribe to channels from the Channel bar interface (Microsoft Developer's Network, 2000).

### ***Disable downloading of site subscription content***

Prevents content from being downloaded from Web sites that users have subscribed to.

When users make Web pages available for offline viewing, they can view content when their computer is not connected to the Internet.

If you enable this policy, content will not be downloaded from Web sites that users have subscribed to. However, synchronization with the Web pages will still occur to determine if any content has been updated since the last time the user synchronized with or visited the page.

If you disable this policy or do not configure it, content will not be prevented from being downloaded.

The "Disable downloading of site subscription content" policy and the "Hide Favorites menu" policy (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer) take precedence over this policy. If either policy is enabled, this policy is ignored (Microsoft Developer's Network, 2000).

### ***Disable editing and scheduling of scheduled groups***

Prevents users from adding, editing, or removing schedules for offline viewing of Web pages and groups of Web pages that users have subscribed to.

A subscription group is a favorite Web page plus the Web pages it links to.

If you enable this policy, the Add, Remove, and Edit buttons on the Schedule tab in the Web page Properties dialog box are dimmed. To display this tab, users click the Tools menu, click Synchronize, select a Web page, click the Properties button, and then click the Schedule tab.

If you disable this policy or do not configure it, users can add, remove, and edit schedules for Web sites and groups of Web sites.

The "Disable editing schedules for offline pages" policy and the "Hide Favorites menu" policy (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer) take precedence over this policy. If either policy is enabled, this policy is ignored (Microsoft Developer's Network, 2000).

### ***Subscription limit***

Restricts the amount of information downloaded for offline viewing.

If you enable this policy, you can set limits to the size and number of pages that users can download. If users attempt to exceed the number of subscriptions, a prompt will appear that states that they cannot set up more Web sites for offline viewing.

If you disable this policy or do not configure it, then users can determine the amount of content that is searched for new information and downloaded.

Caution: Although the Maximum Number of Offline Pages option determines how many levels of a Web site are searched for new information, it does not change the user interface in the Offline Favorites wizard.

Note: The begin and end times for downloading are measured in minutes after midnight. The Maximum Offline Page Crawl Depth

setting specifies how many levels of a Web site are searched for new information (Microsoft Developer's Network, 2000).

(31) Browser Menus

***File menu: Disable Save as... menu option***

Prevents users from saving Web pages from the browser File menu to their hard disk or to a network share.

If you enable this policy, the Save As command on the File menu will be removed.

If you disable this policy or do not configure it, users can save Web pages for later viewing.

This policy takes precedence over the "File Menu: Disable Save As Web Page Complete" policy, which prevents users from saving the entire contents that are displayed or run from a Web Page, such as graphics, scripts, and linked files, but does not prevent users from saving the text of a Web page.

Caution: If you enable this policy, users are not prevented from saving Web content by pointing to a link on a Web page, clicking the right mouse button, and then clicking Save Target As (Microsoft Developer's Network, 2000).

***File menu: Disable New menu option***

Prevents users from opening a new browser window from the File menu.

If this policy is enabled, users cannot open a new browser window by clicking the File menu, pointing to the New menu, and then clicking Window. The user interface is not changed, but a new window will not be opened, and users will be informed that the command is not available.

If you disable this policy or do not configure it, users can open a new browser window from the File menu.

Caution: This policy does not prevent users from opening a new browser window by right clicking, and then clicking the Open in New Window command. To prevent users from using the shortcut menu to open new browser windows, you should also set the "Disable Open in New Window

menu option" policy, which disables this command on the shortcut menu, or the "Disable context menu" policy, which disables the entire shortcut menu (Microsoft Developer's Network, 2000).

***File menu: Disable Open menu option***

Prevents users from opening a file or Web page from the File menu in Internet Explorer.

If you enable this policy, the Open dialog box will not appear when users click the Open command on the File menu. If users click the Open command, they will be notified that the command is not available.

If you disable this policy or do not configure it, users can open a Web page from the browser File menu.

Caution: This policy does not prevent users from right-clicking a link on a Web page, and then clicking the Open or Open in New Window command. To prevent users from opening Web pages by using the shortcut menu, set the "Disable Open in New Window menu option" policy, which disables this command on the shortcut menu, or the "Disable context menu" policy, which disables the entire shortcut menu (Microsoft Developer's Network, 2000).

***File menu: Disable Save as Web Page Complete***

Prevents users from saving the complete contents that are displayed on or run from a Web page, including the graphics, scripts, linked files, and other elements. It does not prevent users from saving the text of a Web page.

If you enable this policy, the Web Page, Complete file type option will be removed from the Save as Type drop-down box in the Save Web Page dialog box. Users can still save Web pages as hypertext markup language (HTML) files or as text files, but graphics, scripts, and other elements are not saved. To display the Save Web Page dialog box, users click the File menu, and then click the Save As command.

If you disable this policy or do not configure it, users can save all elements on a Web page.



The "File menu: Disable Save As... menu option" policy, which removes the Save As command, takes precedence over this policy. If it is enabled, this policy is ignored (Microsoft Developer's Network, 2000).

***File menu: Disable closing browser and explorer windows***

Prevents users from closing Internet Explorer and Windows Explorer.

If you enable this policy, the Close command on the File menu will appear dimmed.

If you disable this policy or do not configure it, users are not prevented from closing the browser or Windows Explorer.

Note: The X button in the top right corner of the program will not work; if users click the X button, they will be informed that the command is not available (Microsoft Developer's Network, 2000).

***View menu: Disable Source menu option***

Prevents users from viewing the HTML source of Web pages by clicking the Source command on the View menu.

If you enable this policy, the Source command on the View menu will appear dimmed.

If you disable this policy or do not configure it, then users can view the HTML source of Web pages from the browser View menu.

Caution: This policy does not prevent users from viewing the HTML source of a Web page by right-clicking a Web page to open the shortcut menu, and then clicking View Source. To prevent users from viewing the HTML source of a Web page from the shortcut menu, set the "Disable context menu" policy, which disables the entire shortcut menu (Microsoft Developer's Network, 2000).

***View menu: Disable Full Screen menu option***

Prevents users from displaying the browser in full-screen (kiosk) mode, without the standard toolbar.

If you enable this policy, the Full Screen command on the View menu will appear dimmed, and pressing F11 will not display the browser in a full screen.

If you disable this policy or do not configure it, users can display the browser in a full screen.

This policy is intended to prevent users from displaying the browser without toolbars, which might be confusing for some beginning users (Microsoft Developer's Network, 2000).

### ***Hide Favorites menu***

Prevents users from adding, removing, or editing the list of Favorite links.

The Favorites list is a way to store popular links for future use.

If you enable this policy, the Favorites menu is removed from the interface, and the Favorites button on the browser toolbar appears dimmed. The Add to Favorites command on the shortcut menu is disabled; when users click it, they are informed that the command is unavailable.

If you disable this policy or do not configure it, users can manage their Favorites list.

This policy is intended to ensure that users maintain consistent lists of favorites across your organization.

Note: If you enable this policy, users also cannot click Synchronize on the Tools menu to manage their favorite links that are set up for offline viewing (Microsoft Developer's Network, 2000).

### ***Tool menu: Disable Internet Options... menu option***

Prevents users from opening the Internet Options dialog box from the Tools menu in Internet Explorer.

If you enable this policy, users cannot change their Internet options, such as default home page, cache size, and connection and proxy settings, from the browser Tools menu. When users click the Internet Options command on the Tools menu, they are informed that the command is unavailable.

If you disable this policy or do not configure it, users can change their Internet settings from the browser Tools menu.

Caution: This policy does not prevent users from viewing and changing Internet settings by clicking the Internet Options icon in Windows Control Panel.

Also, see policies for Internet options in the \Administrative Templates\Windows Components\Internet Explorer and in \Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel folders (Microsoft Developer's Network, 2000).

***Help menu: Remove “Tip of the Day” menu option***

Prevents users from viewing or changing the Tip of the Day interface in Internet Explorer.

If you enable this policy, the Tip of the Day command is removed from the Help menu.

If you disable this policy or do not configure it, users can enable or disable the Tip of the Day, which appears at the bottom of the browser (Microsoft Developer's Network, 2000).

***Help menu: Remove “For Netscape Users” menu option***

Prevents users from displaying tips for users who are switching from Netscape.

If you enable this policy, the For Netscape Users command is removed from the Help menu.

If you disable this policy or do not configure it, users can display content about switching from Netscape by clicking the For Netscape Users command on the Help menu.

Caution: Enabling this policy does not remove the tips for Netscape users from the Internet Explorer Help file (Microsoft Developer's Network, 2000).

***Help menu: Remove Tour menu option***

Prevents users from running the Internet Explorer Tour from the Help menu in Internet Explorer.

If you enable this policy, the Tour command is removed from the Help menu.

If you disable this policy or do not configure it, users can run the tour from the Help menu (Microsoft Developer's Network, 2000).

***Help menu: Remove "Send feedback" menu option***

Prevents users from sending feedback to Microsoft by clicking the Send Feedback command on the Help menu.

If you enable this policy, the Send Feedback command is removed from the Help menu.

If you disable this policy or do not configure it, users can fill out an Internet form to provide feedback about Microsoft products (Microsoft Developer's Network, 2000).

***Disable context menu***

Prevents the shortcut menu from appearing when users click the right mouse button while using the browser.

If you enable this policy, the shortcut menu will not appear when users point to a Web page, and then click the right mouse button.

If you disable this policy or do not configure it, users can use the shortcut menu.

This policy can be used to ensure that the shortcut menu isn't used as an alternate method of running commands that have been removed from other parts of the interface (Microsoft Developer's Network, 2000).

***Disable open in new window menu option***

Prevents using the shortcut menu to open a link in a new browser window.

If you enable this policy, users cannot point to a link, click the right mouse button, and then click the Open in New Window command.

If you disable this policy or do not configure it, users can open a Web page in a new browser window by using the shortcut menu.

This policy can be used in coordination with the "File menu: Disable New menu option" policy, which prevents users from opening the browser in a new window by clicking the File menu, pointing to New, and then clicking Window.

Note: When users click the Open in New Window command, the link will not open in a new

window and they will be informed that the command is not available (Microsoft Developer's Network, 2000).

***Disable save this program to disk option***

Prevents users from saving a program or file that Internet Explorer has downloaded to the hard disk.

If you enable this policy, users cannot save a program to disk by clicking the Save This Program to Disk command while attempting to download a file. The file will not be downloaded and users will be informed that the command is not available.

If you disable this policy or do not configure it, users can download programs from their browsers (Microsoft Developer's Network, 2000).

(32) Toolbars

***Disable customizing browser toolbar buttons***

Prevents users from determining which buttons appear on the Internet Explorer and Windows Explorer standard toolbars.

If you enable this policy, the Customize command on the Toolbars submenu of the View menu will be removed.

If you disable this policy or do not configure it, users can customize which buttons appear on the Internet Explorer and Windows Explorer toolbars.

This policy can be used in coordination with the "Disable customizing browser toolbars" policy, which prevents users from determining which toolbars are displayed in Internet Explorer and Windows Explorer (Microsoft Developer's Network, 2000).

***Disable customizing browser toolbars***

Prevents users from determining which toolbars are displayed in Internet Explorer and Windows Explorer.

If you enable this policy, the list of toolbars, which users can display by clicking the View menu

and then pointing to the Toolbars command, will appear dimmed.

If you disable this policy or do not configure it, users can determine which toolbars are displayed in Windows Explorer and Internet Explorer.

This policy can be used in coordination with the "Disable customizing browser toolbar buttons" policy, which prevents users from adding or removing toolbars from Internet Explorer (Microsoft Developer's Network, 2000).

### ***Configure toolbar buttons***

Specifies which buttons will be displayed on the standard toolbar in Internet Explorer.

If you enable this policy, you can specify whether or not each button will be displayed by selecting or clearing the check boxes for each button.

If you disable this policy or do not configure it, the standard toolbar will be displayed with its default settings, unless users customize it. (Microsoft Developer's Network, 2000).

(33)

Persistence Behavior

### ***File size limits for local machine zones***

Limits the amount of storage that a page or site using the DHTML Persistence behavior can use for the Local Computer security zone.

If you enable this policy, you can specify the persistence storage amount per domain or per document for this security zone.

If you disable this policy or do not configure it, you cannot set this limit.

Note: This setting does not appear in the user interface (Microsoft Developer's Network, 2000).

### ***File size limits for Intranet zone***

Limits the amount of storage that a page or site using the DHTML Persistence behavior can use for the Local Intranet security zone.

If you enable this policy, you can specify the persistence storage amount per domain or per document for this security zone.

If you disable this policy or do not configure it, you cannot set this limit.

Note: This setting does not appear in the user interface (Microsoft Developer's Network, 2000).

***File size limits for trusted sites zone***

Limits the amount of storage that a page or site using the DHTML Persistence behavior can use for the Trusted Sites security zone.

If you enable this policy, you can specify the persistence storage amount per domain or per document for this security zone.

If you disable this policy or do not configure it, you cannot set this limit.

Note: This setting does not appear in the user interface (Microsoft Developer's Network, 2000).

***File size limits for Internet zone***

Limits the amount of storage that a page or site using the DHTML Persistence behavior can use for the Internet security zone.

If you enable this policy, you can specify the persistence storage amount per domain or per document for this security zone.

If you disable this policy or do not configure it, you cannot set this limit.

Note: This setting does not appear in the user interface (Microsoft Developer's Network, 2000).

**(i) File size limits for restricted sites zone**

(ii) Limits the amount of storage that a page or site using the DHTML Persistence behavior can use for the Restricted Sites security zone.

(iii) If you enable this policy, you can specify the persistence storage amount per domain or per document for this security zone.

(iv) If you disable this policy or do not configure it, you cannot set this limit.

**(v)** Note: This setting does not appear in the user interface (Microsoft Developer's Network, 2000).

(34) Administrator Approval Controls

***Media Player***

Designates the Media Player ActiveX control as administrator approved.

This control is used for playing sounds, videos, and other media.

If you enable this policy, this control can be run in security zones in which you specify that administrator-approved controls can be run.

If you disable this policy or do not configure it, this control will not be designated as administrator approved.

To specify how administrator-approved controls are handled for each security zone, carry out the following steps:

1. In Group Policy, click User Configuration, click Internet Explorer Maintenance, and then click Security.

2. Double-click Security Zones and Content Ratings, click Import the Current Security Zones Settings, and then click Modify Settings.

3. Select the content zone in which you want to manage ActiveX controls, and then click Custom Level.



4. In the Run ActiveX Controls and Plug-ins area, click Administrator Approved (Microsoft Developer's Network, 2000).

### ***Menu controls***

Designates a set of Microsoft ActiveX controls used to manipulate pop-up menus in the browser as administrator approved.

If you enable this policy, these controls can be run in security zones in which you specify that administrator-approved controls can be run.

If you disable this policy or do not configure it, these controls will not be designated as administrator approved.

To specify a control as administrator approved, click Enabled, and then select the check box for the control:

- MCSiMenu - enables Web authors to control the placement and appearance of Windows pop-up menus on Web pages

- Popup Menu Object - enables Web authors to add pop-up menus to Web pages

To specify how administrator-approved controls are handled for each security zone, carry out the following steps:

1. In Group Policy, click User Configuration, click Internet Explorer Maintenance, and then click Security.

2. Double-click Security Zones and Content Ratings, click Import the Current Security Zones Settings, and then click Modify Settings.

3. Select the content zone in which you want to manage ActiveX controls, and then click Custom Level.

4. In the Run ActiveX Controls and Plug-ins area, click Administrator Approved (Microsoft Developer's Network, 2000).

### ***Microsoft agent***

Designates the Microsoft Agent ActiveX control as administrator approved.

Microsoft Agent is a set of software services that supports the presentation of software agents as interactive personalities within the Microsoft Windows interface.

If you enable this policy, this control can be run in security zones in which you specify that administrator-approved controls can be run.

If you disable this policy or do not configure it, these controls will not be designated as administrator approved.

To specify how administrator-approved controls are handled for each security zone, carry out the following steps:

1. In Group Policy, click User Configuration, click Internet Explorer Maintenance, and then click Security.
2. Double-click Security Zones and Content Ratings, click Import the Current Security Zones Settings, and then click Modify Settings.
3. Select the content zone in which you want to manage ActiveX controls, and then click Custom Level.
4. In the Run ActiveX Controls and Plug-ins area, click Administrator Approved (Microsoft Developer's Network, 2000).

### ***Microsoft chat***

Designates the Microsoft Chat ActiveX control as administrator approved.

This control is used by Web authors to build text- and graphical-based Chat communities for real-time conversations on the Web.

If you enable this policy, this control can be run in security zones in which you specify that administrator-approved controls can be run.

If you disable this policy or do not configure it, this control will not be designated as administrator approved.

To specify how administrator-approved controls are handled for each security zone, carry out the following steps:

1. In Group Policy, click User Configuration, click Internet Explorer Maintenance, and then click Security.
2. Double-click Security Zones and Content Ratings, click Import the Current Security Zones Settings, and then click Modify Settings.
3. Select the content zone in which you want to manage ActiveX controls, and then click Custom Level.

4. In the Run ActiveX Controls and Plug-ins area, click Administrator Approved (Microsoft Developer's Network, 2000).

***Microsoft survey control***

Designates the Microsoft Survey Control as administrator approved (Microsoft Developer's Network, 2000).

***Shockwave flash***

Designates Shockwave Flash Director as administrator approved (Microsoft Developer's Network, 2000).

***Netshow file transfer control***

Designates the Netshow file transfer control as administrator approved (Microsoft Developer's Network, 2000).

***DHTML edit control***

Designates the DHTML Edit control as administrator approved (Microsoft Developer's Network, 2000).

***Microsoft scriptlet component***

***Carpaint***

Designates the Microsoft Network (MSN) Carpoint automatic pricing control as administrator approved.

This control enables enhanced pricing functionality on the Carpoint Web site, where users can shop for and obtain information about vehicles.

If you enable this policy, this control can be run in security zones in which you specify that administrator-approved controls can be run.

If you disable this policy or do not configure it, this control will not be designated as administrator approved.

To specify how administrator-approved controls are handled for each security zone, carry out the following steps:

1. In Group Policy, click User Configuration, click Internet Explorer Maintenance, and then click Security.

2. Double-click Security Zones and Content Ratings, click Import the Current Security Zones Settings, and then click Modify Settings.

3. Select the content zone in which you want to manage ActiveX controls, and then click Custom Level.

4. In the Run ActiveX Controls and Plug-ins area, click Administrator Approved (Microsoft Developer's Network, 2000).

### ***Investor***

Designates a set of Microsoft Network (MSN) Investor controls as administrator approved.

These controls enable users to view updated lists of stocks on their Web pages.

If you enable this policy, these controls can be run in security zones in which you specify that administrator-approved controls can be run.

If you disable this policy or do not configure it, these controls will not be designated as administrator approved.

Select the check boxes for the controls that you want to designate as administrator approved.

To specify how administrator-approved controls are handled for each security zone, carry out the following steps:

1. In Group Policy, click User Configuration, click Internet Explorer Maintenance, and then click Security.

2. Double-click Security Zones and Content Ratings, click Import the Current Security Zones Settings, and then click Modify Settings.

3. Select the content zone in which you want to manage ActiveX controls, and then click Custom Level.

4. In the Run ActiveX Controls and Plug-ins area, click Administrator Approved (Microsoft Developer's Network, 2000).

### ***MSNBC***

Designates a set of MSNBC controls as administrator approved.

These controls enable enhanced browsing of news reports on the MSNBC Web site.

If you enable this policy, these controls can be run in security zones in which you specify that administrator-approved controls can be run.

If you disable this policy or do not configure it, these controls will not be designated as administrator approved.

Select the check boxes for the controls that you want to designate as administrator approved.

To specify how administrator-approved controls are handled for each security zone, carry out the following steps:

1. In Group Policy, click User Configuration, click Internet Explorer Maintenance, and then click Security.

2. Double-click Security Zones and Content Ratings, click Import the Current Security Zones Settings, and then click Modify Settings.

3. Select the content zone in which you want to manage ActiveX controls, and then click Custom Level.

4. In the Run ActiveX Controls and Plug-ins area, click Administrator Approved (Microsoft Developer's Network, 2000).

## ***Windows Explorer***

### ***Enable classic shell***

Disables Active Desktop, Web view, and thumbnail views. Also, users cannot configure their system to open items by single-clicking (such as in Mouse in Control Panel). As a result, the user interface looks and operates like the interface for Windows NT 4.0 and users cannot restore the new features.

Note: This policy takes precedence over the "Enable Active Desktop" policy. If both policies are enabled, Active Desktop is disabled.

Also, see the "Disable Active Desktop" policy in User Configuration\Administrative Templates\Desktop\Active Desktop and the "Remove the Folder Options menu item from the Tools menu" policy in User Configuration\Administrative Templates\Windows Components\Windows Explorer (Microsoft Developer's Network, 2000).

### ***Removes the folder options menu item from the tools menu***

Removes the Folder Options item from all Windows Explorer menus and removes the Folder Options item from Control Panel. As a result, users cannot use the Folder Options dialog box.

The Folder Options dialog box lets users set many properties of Windows Explorer, such as Active Desktop, Web view, Offline Files, hidden system files, and file types.

Also, see the "Enable Active Desktop" policy in User Configuration\Administrative Templates\Desktop\Active Desktop and the "Disable user configuration of Offline Files" policy in User Configuration\Administrative Templates\Network\Offline Files (Microsoft Developer's Network, 2000).

***Remove file menu form windows explorer***

Removes the File menu from My Computer and Windows Explorer.

This policy does not prevent users from using other methods to perform tasks available on the File menu (Microsoft Developer's Network, 2000).

***Remove "Map network drive" and "Disconnect network drive"***

Prevents users from using Windows Explorer or My Network Places to connect to other computers or to close existing connections.

If you enable this policy, the system removes the Map Network Drive and Disconnect Network Drive commands from the toolbar and Tools menus in Windows Explorer and My Network Places and from menus that appear when you right-click the Windows Explorer or My Network Places icons. It also removes the Add Network Place option from My Network Places.

This policy does not prevent users from connecting to another computer by typing the name of a shared folder in the Run dialog box (Microsoft Developer's Network, 2000).

***Remove search button for windows explorer***

Removes the Search button from the Windows Explorer toolbar.

This policy removes the Search button from the Standard Buttons toolbar that appears in Windows Explorer and other programs that use the Windows Explorer window, such as My Computer and My Network Places.

It does not remove the Search button or affect any search features of Internet browser windows, such as the Internet Explorer window.

This policy does not affect the Search items on the Windows Explorer context menu or on the Start menu. To remove Search from the Start menu, use the "Remove Search menu from Start menu" policy (in User Configuration\Administrative Templates\Start Menu &

Taskbar). To hide all context menus, use the "Disable Windows Explorer's default context menu" policy (Microsoft Developer's Network, 2000).

***Disable window explorer's default context menu***

Removes shortcut menus from the desktop and Windows Explorer. Shortcut menus appear when you right-click an item.

If you enable this policy, menus do not appear when you right-click the desktop or when you right-click the items in Windows Explorer. This policy does not prevent users from using other methods to issue commands available on the shortcut menus (Microsoft Developer's Network, 2000).

***Hides the manage item on the windows explorer context menu***

Removes the Manage item from the Windows Explorer context menu. This context menu appears when you right-click Windows Explorer or My Computer.

The Manage item opens Computer Management (Compmgmt.msc), a console tool which includes many of the primary Windows 2000 administrative tools, such as Event Viewer, Device Manager, and Disk Management. You must be an administrator to use many of the features of these tools.

This policy does not remove the Computer Management item from the Start Menu (Start, Programs, Administrative Tools, Computer Management), nor does it prevent users from using other methods to start Computer Management.

Tip: To hide all context menus, use the "Disable Windows Explorer's default context menu" policy (Microsoft Developer's Network, 2000).

***Only allow approved shell extensions***

Directs Windows to start only the user interface extensions that the system security or the user have approved.

When the system detects that the user is downloading an external program that runs as part of the Windows user interface, the system searches for a digital certificate or requests that the user approve the action. If you enable this policy, Windows only starts approved programs.

This policy is designed to protect the system from damage from programs that do not operate correctly or are intended to cause harm.

Note: To view the approved user interface extensions for a system, start a registry editor (Regedt32 or Regedit). The system stores entries representing approved user interface extensions on a system in the following registry key:

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved  
(Microsoft Developer's Network, 2000)

### ***Do not track shell shortcuts during roaming***

Determines whether Windows traces shortcuts back to their sources when it cannot find the target on the user's system.

Shortcut files typically include an absolute path to the original target file as well as the relative path to the current target file. When the system cannot find the file in the current target path, then, by default, it searches for the target in the original path. If the shortcut has been copied to a different computer, the original path might lead to a network computer, including external resources, such as an Internet server.

If you enable this policy, Windows only searches the current target path. It does not search for the original path even when it cannot find the target file in the current target path (Microsoft Developer's Network, 2000).

### ***Hide these specified drives in My computer***

Removes the icons representing selected hard drives from My Computer, Windows Explorer, and My Network Places. Also, the drive letters representing the selected drives do not appear in the standard Open dialog box.

To use this policy, select a drive or combination of drives from the drop-down list. To display all drives, disable this policy or select the "Do not restrict drives" option from the drop-down list.

Note: This policy removes the drive icons. Users can still gain access to drive contents by using other methods, such as by typing the path to a directory on the drive in the Map Network Drive dialog box, in the Run dialog box, or in a command window.

Also, this policy does not prevent users from using programs to access these drives or their contents. And, it does not prevent users from using the Disk Management



snap-in to view and change drive characteristics (Microsoft Developer's Network, 2000).

### ***Prevents access to drives from My computer***

Prevents users from using My Computer to gain access to the content of selected drives.

If you enable this policy, users cannot view the contents of the selected drives in My Computer, Windows Explorer, or My Network Places. Also, they cannot use the Run dialog box, the Map Network Drive dialog box, or the Dir command to view the directories on these drives.

To use this policy, select a drive or combination of drives from the drop-down list. To allow access to all drive directories, disable this policy or select the "Do not restrict drives" option from the drop-down list.

Note: The icons representing the specified drives still appear in My Computer, but if users double-click the icons, a message appears explaining that a policy prevents the action.

Also, this policy does not prevent users from using programs to access local and network drives. And, it does not prevent them from using the Disk Management snap-in to view and change drive characteristics (Microsoft Developer's Network, 2000).

### ***Hide hardware tab***

Removes the Hardware tab.

This policy removes the Hardware tab from Mouse, Keyboard, and Sounds and Multimedia in Control Panel. It also removes the Hardware tab from the Properties dialog box for all local drives, including hard drives, floppy disk drives, and CD-ROM drives. As a result, users cannot use the Hardware tab to view or change the device list or device properties, or use the Troubleshoot button to resolve problems with the device (Microsoft Developer's Network, 2000).

### ***Disable UI to change menu animation settings***

Prevents users from selecting the option to animate the movement of windows, menus, and lists.

If you enable this policy, the "Use transition effects for menus and tooltips" option in Display in Control Panel is disabled.

Effects, such as animation, are designed to enhance the user's experience but might be confusing or distracting to some users (Microsoft Developer's Network, 2000).

### ***Disable UI to change keyboard navigation indicator settings***

Disables the "Hide keyboard navigation indicators until I use the ALT key" option in Display in Control Panel.

When this Display Properties option is selected, the underlining that indicates a keyboard shortcut character (hot key) does not appear on menus until you press ALT.

Effects, such as transitory underlines, are designed to enhance the user's experience but might be confusing or distracting to some users (Microsoft Developer's Network, 2000).

### ***Disable DFS tab***

Removes the DFS tab from Windows Explorer.

This policy removes the DFS tab from Windows Explorer and from other programs that use the Windows Explorer browser, such as My Computer. As a result, users cannot use this tab to view or change the properties of the Distributed File System (DFS) shares available from their computer.

This policy does not prevent users from using other methods to configure DFS (Microsoft Developer's Network, 2000).

### ***No "Computers near me" in My network place***

Removes computers in the user's workgroup and domain from lists of network resources in Windows Explorer and My Network Places.

If you enable this policy, the system removes the "Computers Near Me" option and the icons representing nearby computers from My Network Places. This policy also removes these icons from the Map Network Drive browser.

This policy does not prevent users from connecting to computers in their workgroup or domain by other commonly used methods, such as typing the share name in the Run dialog box or the Map Network Drive dialog box.

To remove network computers from lists of network resources, use the "No Entire Network in My Network Places" policy (Microsoft Developer's Network, 2000).

### ***No "Entire network" in My network place***

Removes all computers outside of the user's workgroup or local domain from lists of network resources in Windows Explorer and My Network Places.

If you enable this policy, the system removes the Entire Network option and the icons representing networked computers from My Network Places and from the browser associated with the Map Network Drive option.

This policy does not prevent users from viewing or connecting to computers in their workgroup or domain. It also does not prevent users from connecting to remote computers by other commonly used methods, such as by typing the share name in the Run dialog box or the Map Network Drive dialog box.

To remove computers in the user's workgroup or domain from lists of network resources, use the "No 'Computers Near Me' in My Network Places" policy (Microsoft Developer's Network, 2000).

### ***Maximum number of recent documents***

Determines how many shortcuts the system can display in the Documents menu on the Start menu.

The Documents menu contains shortcuts to the non-program files the user has most recently opened. By default, the system displays shortcuts to the 15 most recently opened documents (Microsoft Developer's Network, 2000).

### ***Do not request alternate credentials***

Prevents users from submitting alternate logon credentials to install a program.

This policy suppresses the "Install Program As Other User" dialog box for local and network installations. This dialog box, which prompts the current user for the user name and password of an administrator, appears when users who are not administrators try to install programs locally on their computers. This policy allows administrators who have logged on as regular users to install programs without logging off and logging on again using their administrator credentials.

There are many programs can be installed only by an administrator. If you enable this policy and a user does not have sufficient permissions to install a program, the installation continues with the current user's logon credentials. As a result, the installation might fail, or it might complete but not include all features. Or it might appear to complete successfully, but the installed program might not operate correctly.

If you disable this policy, or do not configure it, the "Install Program As Other User" dialog box appears whenever users install programs locally on the computer.

By default, users are not prompted for alternate logon credentials when installing programs from a network share. If enabled, this policy overrides the "Request credentials for network installations" policy (Microsoft Developer's Network, 2000).

***Request credentials for network installations***

Prompts users for alternate logon credentials during network-based installations.

This policy displays the "Install Program As Other User" dialog box even when a program is being installed from files on a network computer across a local area network connection.

If you disable this policy or do not configure it, this dialog box appears only when users are installing programs from local media.

The "Install Program as Other User" dialog box prompts the current user for the user name and password of an administrator. This policy allows administrators who have logged on as regular users to install programs without logging off and logging on again using their administrator credentials.

If the dialog box does not appear, the installation proceeds with the current user's permissions. If these permissions are not sufficient, the installation might fail, or it might complete but not include all features. Or, it might appear to complete successfully, but the installed program might not operate correctly.

Note: If enabled, the "Do not request alternate credentials" policy takes precedence over the setting for this policy. When that policy is enabled, users are not prompted for alternate logon credentials on any installation (Microsoft Developer's Network, 2000).

(35) Common Open File Dialog

***Hide the common dialog places bar***

Removes the shortcut bar from the Open dialog box.

This policy, and others in this folder, lets you remove new features added in Windows 2000, so that the Open dialog box looks like it did in Windows NT 4.0 and earlier. These policies only affect programs that use the standard Open dialog box provided to developers of Windows programs.

To see an example of the standard Open dialog box, run Notepad and, from the File menu, click Open (Microsoft Developer's Network, 2000).

***Hide the common dialog back button***

Removes the Back button from the Open dialog box.

This policy, and others in this folder, lets you remove new features added in Windows 2000, so that the Open dialog box looks like it did in Windows NT 4.0 and earlier. These policies only affect programs that use the standard Open dialog box provided to developers of Windows programs.

To see an example of the standard Open dialog box, run Notepad and, from the File menu, click Open (Microsoft Developer's Network, 2000).

***Hide the dropdown list of recent files***

Removes the list of most recently used files from the Open dialog box.

If you disable this policy or do not configure it, the "File name" field includes a dropdown list of recently used files. If you enable this policy, the "File name" field is a simple text box. Users must browse directories to find a file or type a file name in the text box.

This policy, and others in this folder, lets you remove new features added in Windows 2000, so that the Open dialog box looks like it did in Windows NT 4.0 and earlier. These policies only affect programs that use the standard Open dialog box provided to developers of Windows programs.

To see an example of the standard Open dialog box, run Notepad and, from the File menu, click Open (Microsoft Developer's Network, 2000).

***Microsoft Management Console***

***Restrict the user from entering the author mode***

Prevents users from entering author mode.

This policy prevents users from opening the MMC in author mode, from explicitly opening console files in author mode, and from opening any console files that open in author mode by default.

As a result, users cannot create console files or add or remove snap-ins. Also, because they cannot open author-mode console files, they cannot use the tools that the files contain.

This policy permits users to open MMC user-mode console files, such as those on the Administrative Tools menu in Windows 2000 Server. However, users cannot open a blank MMC console window, on the Start menu. (To open the MMC, click Start, click Run, and type MMC.) Users also cannot open a blank MMC console window from a command prompt.

If you disable this policy or do not configure it, users can enter author mode and open author-mode console files (Microsoft Developer's Network, 2000).

***Restrict the users to the explicitly permitted list of snap-ins***

Lets you selectively permit or prohibit the use of Microsoft Management Console (MMC) snap-ins.

-- If you enable this policy, all snap-ins are prohibited, except those that you explicitly permit. Use this setting if you plan to prohibit use of most snap-ins.

To explicitly permit a snap-in, open the Restricted/Permitted snap-ins policy folder and then enable the policies representing the snap-in you want to permit. If a snap-in policy in the folder is disabled or not configured, the snap-in is prohibited.

-- If you disable this policy or do not configure it, all snap-ins are permitted, except those that you explicitly prohibit. Use this setting if you plan to permit use of most snap-ins.

To explicitly prohibit a snap-in, open the Restricted/Permitted snap-ins policy folder and then disable the policies representing the snap-ins you want to prohibit. If a snap-in policy in the folder is enabled or not configured, the snap-in is permitted.

When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear.

Note: If you enable this policy, and do not enable any policies in the Restricted/Permitted snap-ins folder, users cannot use any MMC snap-ins (Microsoft Developer's Network, 2000).

***Restricted/Permitted Snap-ins***

Permits or prohibits use of this snap-in.

If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.

If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-

ins" policy determines whether this snap-in is permitted or prohibited.

-- If "Restrict users to the explicitly permitted list of snap-ins" is enabled, users cannot use any snap-in except those explicitly permitted.

To explicitly permit use of this snap-in, enable this policy. If this policy is not configured (or disabled), this snap-in is prohibited.

-- If "Restrict users to the explicitly permitted list of snap-ins" is disabled or not configured, users can use any snap-in except those explicitly prohibited.

To explicitly prohibit use of this snap-in, disable this policy. If this policy is not configured (or enabled), the snap-in is permitted.

When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear (Microsoft Developer's Network, 2000).

**All the following snap-ins are affected by this policy**

**(a) Active directory users and computers**

*Active directory sites and services*  
*Active directory domains and trusts*  
*Certificates*  
*Component Services*  
*Computer management*  
*Device manager*  
*Disk Management*  
*Disk Defragmenter*  
*Distributed File System*

**(ii) Event viewer**

*FAX service*  
*Indexing service*  
*Internet Authentication service*  
*Internet information service*  
*IP security*  
*Local users and groups*  
*Performance logs and alerts*  
*QoS admission control*  
*Removable storage management*

***Routing and remote access***  
***Security Configuration and analysis***  
***Security templates***  
***Services***  
***Shared folders***  
***System information***  
***Telephony***  
***Terminal services configuration***  
***VMI control***

*(b) Extension Snap-ins*

Permits or prohibits use of this snap-in.

If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.

If this policy is not configured, then the setting of the "Restrict users to the explicitly permitted list of snap-ins" policy determines whether this snap-in is permitted or prohibited.

-- If "Restrict users to the explicitly permitted list of snap-ins" is enabled, users cannot use any snap-in except those explicitly permitted.

To explicitly permit use of this snap-in, enable this policy. If this policy is not configured (or disabled), this snap-in is prohibited.

-- If "Restrict users to the explicitly permitted list of snap-ins" is disabled or not configured, users can use any snap-in except those explicitly prohibited.

To explicitly prohibit use of this snap-in, disable this policy. If this policy is not configured (or enabled), the snap-in is permitted.

When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear (Microsoft Developer's Network, 2000).



All the following snap-ins are affected by this policy

- (i) Apple Talk Routing
  - Certification Authority*
  - Connection sharing (NAT)*
  - DCOM configuration extension*
  - Device manager*
  - DHCP relay management*
  - Event viewer*
  - IAS Logging*
  - IGMP routing*
  - IPX routing*
  - IPX RIP routing*
  - IPX SAP routing*
  - Logical and mapped drives*
  - OSPF routing*
  - Public Key policies*
  - RAS dial-in*
  - Remote Access*
  - Removable storage*
  - RIP routing*
  - Routing*
  - Send console message*
  - Services dependencies*
  - SMTP Protocol*
  - SNMP*
  - System properties*

(c) *Group Policy*

(a) *Permits or prohibits use of this snap-in.*

(b) *If you enable this policy, the snap-in is permitted. If you disable the policy, the snap-in is prohibited.*

(c) *If this policy is not configured, then the setting of the "Restrict users to the*

*explicitly permitted list of snap-ins" policy determines whether this snap-in is permitted or prohibited.*

(d) -- *If "Restrict users to the explicitly permitted list of snap-ins" is enabled, users cannot use any snap-in except those explicitly permitted.*

(e) *To explicitly permit use of this snap-in, enable this policy. If this policy is not configured (or disabled), this snap-in is prohibited.*

(f) -- *If "Restrict users to the explicitly permitted list of snap-ins" is disabled or not configured, users can use any snap-in except those explicitly prohibited.*

(g) *To explicitly prohibit use of this snap-in, disable this policy. If this policy is not configured (or enabled), the snap-in is permitted.*

When a snap-in is prohibited, it does not appear in the Add/Remove Snap-in window in MMC. Also, when a user opens a console file that includes a prohibited snap-in, the console file opens, but the prohibited snap-in does not appear (Microsoft Developer's Network, 2000).

**All the following snap-ins are affected by this policy**

(i) Group policy snap-in

*Group policy tab for active directory tools*

*Administrative templates (Computers)*

*Administrative templates (Users)*

*Folder Redirection*

*Internet Explorer*

*Maintenance*

*Remote installation service*  
*Scripts (logon/logoff)*  
*Scripts (startup/shutdown)*  
*Security settings*  
*Software installation*  
*(Computers)*  
*Software installation (Users)*

***Task Scheduler***

**(ii) *Hide property pages***

(iii) Prevents users from viewing and changing the properties of an existing task.

(iv) This policy removes the Properties item from the File menu in Scheduled Tasks and from the context menu that appears when you right-click a task. As a result, users cannot change any properties of a task. They can only see the properties that appear in Detail view and in the task preview.

(v) This policy prevents users from viewing and changing characteristics such as the program the task runs, its schedule details, idle time and power management settings, and its security context.

(vi) Note: This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

**(vii)** Tip: This policy affects existing tasks only. To prevent users from changing the properties of newly created tasks, use the "Disable Advanced Menu" policy (Microsoft Developer's Network, 2000).

***Prevent task run or end***

Prevents users from starting and stopping tasks manually.

This policy removes the Run and End Task items from the context menu that appears when you right-click a task. As a result, users cannot start tasks manually or force tasks to end before they are finished.

Note: This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration (Microsoft Developer's Network, 2000).

### ***Disable Drag-and-drop***

Prevents users from adding or removing tasks by moving or copying programs in the Scheduled Tasks folder.

This policy disables the Cut, Copy, Paste, and Paste shortcut items on the context menu and the Edit menu in Scheduled Tasks. It also disables the drag-and-drop features of the Scheduled Tasks folder.

As a result, users cannot add new scheduled tasks by dragging, moving, or copying a document or program into the Scheduled tasks folder.

This policy does not prevent users from using other methods to create new tasks and it does not prevent users from deleting tasks.

Note: This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration (Microsoft Developer's Network, 2000).

### ***Disable new task creation***

Prevents users from creating new tasks.

This policy removes the Add Scheduled Task item that starts the New Task wizard. Also, the system does not respond when users try to move, paste, or drag programs or documents into the Scheduled Tasks folder.

Note: This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Important: This policy does not prevent administrators of a computer from using At.exe to create new tasks or prevent administrators from

submitting tasks from remote computers (Microsoft Developer's Network, 2000).

### ***Disable task deletion***

Prevents users from deleting tasks from the Scheduled Tasks folder.

This policy removes the Delete item from the Edit menu in the Scheduled Tasks folder and from the menu that appears when you right-click a task. Also, the system does not respond when users try to cut or drag a task from the Scheduled Tasks folder.

Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

*Important: This policy does not prevent administrators of a computer from using At.exe to delete tasks (Microsoft Developer's Network, 2000).*

### ***Disable advanced menu***

Prevents users from viewing or changing the properties of newly created tasks.

This policy removes the "Open advanced properties for this task when I click Finish" item from the last page of the Scheduled Task wizard.

This policy prevents users from viewing and changing task characteristics, such as the program the task runs, details of its schedule, idle time and power management settings, and its security context. It is designed to simplify task creation for beginning users.

Note: This policy appears in the Computer Configuration and User Configuration folders. if both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Tip: This policy affects newly created tasks only. To prevent users from changing the properties of existing tasks, use the "Hide Property Pages" policy (Microsoft Developer's Network, 2000).

### ***Prohibit browse***

Limits newly scheduled items on the user's start menu and prevents the user from changing the scheduled program for existing tasks.

This policy removes the Browse button from the Schedule Task wizard and from the Task tab of the properties dialog box for a task. Also, users cannot edit the "Run" box or the "Start in" box that determine the program and path for a task.

As a result, when users create a task, they must select a program from the list in the Scheduled Task wizard, which displays only the tasks that appear on the Start menu and its submenus. Once a task is created, users cannot change the program a task runs.

Important: This policy does not prevent users from creating a new task by pasting or dragging any program into the Scheduled Tasks folder. To prevent this action, use the "Disable Drag-and-Drop" policy.

Note: This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration (Microsoft Developer's Network, 2000).

### ***Windows Installer***

#### ***(viii) Always install with elevated privileges***

(ix) Directs Windows Installer to use system permissions when it installs any program on the system.

(x) This policy extends elevated privileges to all programs. These privileges are usually reserved for programs that have been assigned to the user (offered on the desktop), assigned to the computer (installed automatically), or made available in Add/Remove Programs in Control Panel. This policy lets users install programs that require access to directories that the user might not have permission to view or change, including directories on highly restricted computers.

(xi) If you disable this policy or do not configure it, the system applies the current

user's permissions when it installs programs that a system administrator does not distribute or offer.

(xii) Note: This policy appears both in the Computer Configuration and User Configuration folders. To make this policy effective, you must enable the policy in both folders.

**(xiii)** Caution: Skilled users can take advantage of the permissions this policy grants to change their privileges and gain permanent access to restricted files and folders. Note that the User Configuration version of this policy is not guaranteed to be secure (Microsoft Developer's Network, 2000).

### ***Search order***

Specifies the order in which Windows Installer searches for installation files.

By default, the Windows Installer searches the network first, then removable media (floppy drive, CD-ROM, or DVD), and finally, the Internet (URL).

To change the search order, enable the policy, and then type the letters representing each file source in the order that you want Windows Installer to search.:

- "n" represents the network;
- "m" represents media;
- "u" represents URL, or the Internet.

To exclude a file source, omit or delete the letter representing that source type (Microsoft Developer's Network, 2000).

### ***Disable rollback***

Prohibits Windows Installer from generating and saving the files it needs to reverse an interrupted or unsuccessful installation.

This policy prevents Windows Installer from recording the original state of the system and sequence of changes it makes during installation. It also prevents Windows Installer from retaining files it intends to delete later. As a result, Windows installer cannot restore the computer to its original state if the installation does not complete.

This policy is designed to reduce the amount of temporary disk space required to install programs. Also, it prevents malicious users from interrupting an installation to gather data about the internal state of the computer or to search secure system files. However, because an incomplete installation can render the system or a program inoperable, do not use this policy unless essential.

This policy appears in the Computer Configuration and User Configuration folders. If the policy is enabled in either folder, it is considered be enabled, even if it is explicitly disabled in the other folder (Microsoft Developer's Network, 2000).

### ***Disable media source for any install***

Prevents users from installing programs from removable media.

If a user tries to install a program from removable media, such as CD-ROMs, floppy disks, and DVDs, a message appears, stating that the feature cannot be found.

This policy applies even when the installation is running in the user's security context.

If you disable this policy or do not configure it, users can install from removable media when the installation is running in their own security context, but only system administrators can use removable media when an installation is running with elevated system privileges, such as installations offered on the desktop or in Add/Remove Programs.

Also, see the "Enable user to use media source while elevated policy" in Computer Configuration\Administrative Templates\Windows Components\Windows Installer (Microsoft Developer's Network, 2000).

## **Start Menu and Taskbar**

### ***Remove user's folder from the start menu***

Hides all folders on the user-specific (top) section of the Start menu. Other items appear, but folders are hidden.

This policy is designed for use with redirected folders. Redirected folders appear on the main (bottom) section of the Start menu. However, the original, user-specific version of the folder still appears on the top section of the Start menu. Because the appearance of two folders with the same name might confuse users, you can use this policy to hide user-specific folders.



Note that this policy hides all user-specific folders, not just those associated with redirected folders.

If you enable this policy, no folders appear on the top section of the Start menu. If users add folders to the Start Menu directory in their user profiles, the folders appear in the directory but not on the Start menu.

If you disable this policy or do not configure it, Windows 2000 displays folders on both sections of the Start menu (Microsoft Developer's Network, 2000).

### ***Disable and remove links to windows update***

Prevents users from connecting to the Windows Update Web site.

This policy blocks user access to the Windows Update Web site at <http://windowsupdate.microsoft.com>. Also, the policy removes the Windows Update hyperlink from the Start Menu and from the Tools menu in Internet Explorer.

Windows Update, the online extension of Windows, offers software updates to keep a user's system up-to-date. The Windows Update Product Catalog determines any system files, security fixes, and Microsoft updates that users need and shows the newest versions available for download (Microsoft Developer's Network, 2000).

### ***Remove common programs group from start menu***

Removes items in the All Users profile from the Programs menu on the Start menu.

By default, the Programs menu contains items from the All Users profile and items from the user's profile. If you enable this policy, only items in the user's profile appear in the Programs menu.

Tip: To see the Program menu items in the All Users profile, on the system drive, go to Documents and Settings\All Users (WINNT)\Start Menu\Programs (Microsoft Developer's Network, 2000).

### ***Remove documents menu from start menu***

Removes the Documents menu from the Start menu.

The Documents menu contains links to the non-program files that users have most recently opened. It appears so that users can easily reopen the documents.

You can use this policy, in coordination with the "Do not keep history of recently opened documents" and "Clear history of recently opened documents on exit" policies in this folder, to customize your policy for managing access to recently opened files (Microsoft Developer's Network, 2000).

### ***Disable programs on setting menu***

Prevents Control Panel, Printers, and Network and Dial-up Connections from running.

This policy removes the Control Panel, Printers, and Network and Dial-up Connection folders from Settings on the Start menu, and from My Computer and Windows Explorer. It also prevents the programs represented by these folders (such as Control.exe) from running.

However, users can still start Control Panel items by using other methods, such as right-clicking the desktop to start Display or right-clicking My Computer to start System (Microsoft Developer's Network, 2000).

### ***Remove networks and dial-up connections from start menu***

Prevents users from running Network and Dial-up Connections.

This policy prevents the Network and Dial-up Connections folder from opening. This policy also removes Network and Dial-up Connections from Settings on the Start menu.

Network and Dial-up Connections still appears in Control Panel and in Windows Explorer, but if users try to start it, a message appears explaining that a policy prevents the action (Microsoft Developer's Network, 2000).

### ***Remove favorites menu from start menu***

Prevents users from adding the Favorites menu to the Start menu.

The Favorites menu does not appear on the Start menu by default. To display the Favorites menu, click Start, point to Settings, click Taskbar & Start Menu, click the Start Menu Options tab, and then, under Start Menu Settings, select Display Favorites. If you enable this policy, the Display Favorites item does not appear in the Start Menu Settings box.

The items that appear in the Favorites menu when you install Windows are preconfigured by the system to appeal to most users. However, users can add and remove items from this menu, and system administrators can create a customized Favorites menu for a user group.

This policy only affects the Start menu. The Favorites item still appears in Windows Explorer and in Internet Explorer (Microsoft Developer's Network, 2000).

### ***Remove search menu from start menu***

Removes the Search item from the Start Menu and disables some Windows Explorer search elements.

This policy removes the Search item from the Start menu and from the context menu that appears when you right-click the

Start menu. Also, the system does not respond when users press the Application key (the key with the Windows logo)+ F.

In Windows Explorer, the Search item still appears on the Standard buttons toolbar, but the system does not respond when the user presses Ctrl + F. Also, Search does not appear in the context menu when you right-click an icon representing a drive or a folder.

This policy affects the specified user interface elements only. It does not affect Internet Explorer and does not prevent the user from using other methods to search (Microsoft Developer's Network, 2000).

#### ***Remove help menu from start menu***

Removes the Help command from the Start menu.

This policy only affects the Start menu. It does not remove the Help menu from Windows Explorer and does not prevent users from running Windows 2000 Help (Microsoft Developer's Network, 2000).

#### ***Remove run menu from start menu***

Removes the Run command from the Start menu and removes the New Task (Run) command from Task Manager. Also, users with extended keyboards can no longer display the Run dialog box by pressing Application key (the key with the Windows logo) + R.

This policy affects the specified interface only. It does not prevent users from using other methods to run programs (Microsoft Developer's Network, 2000).

#### ***Add logoff to start menu***

Adds the "Log Off <username>" item to the Start menu and prevents users from removing it.

If you enable this policy, the Log Off <username> item appears in the Start menu. This policy also removes the Display Logoff item from Start Menu Options. As a result, users cannot remove the Log Off <username> item from the Start Menu.

If you disable this policy or do not configure it, users can use the Display Logoff item to add and remove the Log Off item.

This policy affects the Start menu only. It does not affect the Log Off item on the Windows Security dialog box that appears when you press Ctrl+Alt+Del.

Tip: To add or remove the Log Off item on a computer, click Start, click Settings, click Taskbar & Start Menu, click the Start Menu Options tab and, in the Start Menu Settings box, click Display Logoff (Microsoft Developer's Network, 2000).

#### ***Disable logoff on the start menu***

Removes the "Log Off <username>" item from the Start menu and prevents users from restoring it.

If you enable this policy, the Log Off <username> item does not appear in the Start menu. This policy also removes the Display Logoff item from Start Menu Options. As a result, users cannot restore the Log Off <username> item to the Start Menu.

If you disable this policy or do not configure it, users can use the Display Logoff item to add and remove the Log Off item.

This policy affects the Start menu only. It does not affect the Log Off item on the Windows Security dialog box that appears when you press Ctrl+Alt+Del, and it does not prevent users from using other methods to log off.

Tip: To add or remove the Log Off item on a computer, click Start, click Settings, click Taskbar & Start Menu, click the Start Menu Options tab and, in the Start Menu Settings box, click Display Logoff (Microsoft Developer's Network, 2000).

### ***Disable and remove the shutdown command***

Prevents users from shutting down or restarting Windows.

This policy removes the Shut Down option from the Start menu and disables the Shut Down button on the Windows Security dialog box, which appears when you press CTRL+ALT+DEL.

This policy prevents users from using the Windows user interface to shut down the system, although it does not prevent them from running programs that shut down Windows.

If you disable this policy or do not configure it, the Shut Down menu option appears, and the Shut Down button is enabled (Microsoft Developer's Network, 2000).

### ***Disable drag-and-drop context menus from the start menu***

Prevents users from using the drag-and-drop method to reorder or remove items on the Start menu. Also, it removes context menus from the Start menu.

If you disable this policy or do not configure it, users can remove or reorder Start menu items by dragging and dropping the item. They can display context menus by right-clicking a Start menu item.

This policy does not prevent users from using other methods of customizing the Start menu or performing the tasks available from the context menus (Microsoft Developer's Network, 2000).

### ***Disable changes to taskbar and start menu settings***

Removes the Taskbar & Start Menu item from Settings on the Start menu. This policy also prevents the user from opening the Taskbar Properties dialog box.

If the user right-clicks the taskbar and then clicks Properties, a message appears explaining that a policy prevents the action (Microsoft Developer's Network, 2000).

***Disable context menus for the taskbar***

Hides the menus that appear when you right-click the taskbar and items on the taskbar, such as the Start button, the clock, and the taskbar buttons.

This policy does not prevent users from using other methods to issue the commands that appear on these menus (Microsoft Developer's Network, 2000).

***Do not keep history of recently opened document***

Prevents the system from saving shortcuts to documents the user has most recently opened.

By default, the system saves a shortcut to each of the non-program files the user most recently opened and displays the shortcuts on the Start menu under Documents. The shortcuts let users easily review and restart recently used documents.

If you enable this policy, the system does not save shortcuts to the Documents menu.

You can use this policy, in coordination with the "Remove Documents menu from Start Menu" and "Clear history of recently opened documents on exit" policies in this folder, to customize your policy for managing access to recently opened files.

If you enable this policy and do not select the "Remove Documents menu from Start Menu" policy, the Documents menu appears on the Start menu, but it is empty (Microsoft Developer's Network, 2000).

***Clear history of recently opened documents on exit***

Directs the system to delete the contents of the Documents menu on the Start menu when the user logs off.

The Documents menu contains shortcuts to the non-program files the user opened most recently.

If you enable this policy, the Documents menu is always empty when the user logs on. Otherwise, when the user logs on again, the Documents menu appears just as it did when the user logged off.

You can use this policy, in coordination with the "Remove Documents menu from Start Menu" and "Do not keep history of recently opened documents" policies in this folder to customize your policy for managing access to recently opened files. The system uses this policy only when neither of these related policies are selected (Microsoft Developer's Network, 2000).

***Disable personalized menus***

Disables personalized menus.

Windows 2000 personalizes long menus by moving recently used items to the top of the menu and hiding items that have not been used recently. Users can display the hidden items by clicking an arrow to extend the menu.

If you enable this policy, the system does not personalize menus. All menu items appear and remain in standard order. Also, this policy removes the "Use Personalized Menus" option so users do not try to change the setting while a policy is in effect.

Note: Personalized menus require user tracking. If you enable the "Disable user tracking" policy, the system disables user tracking and personalized menus, and ignores this policy.

Tip: To disable personalized menus without setting a policy, click Start, click Settings, click Taskbar & Start Menu, and, on the General tab, clear the "Use Personalized Menus" option (Microsoft Developer's Network, 2000).

### ***Disable user tracking***

Disables user tracking.

This policy prevents the system from tracking the programs users run, the paths they navigate, and the documents they open. The system uses this information to customize Windows features, such as personalized menus.

If you enable this policy, the system does not track these user actions. The system disables customized features that require user tracking information, including personalized menus (Microsoft Developer's Network, 2000).

### ***Add "Run in separate memory space" check box to run dialog box***

Lets users run a 16-bit program in a dedicated (not shared) Virtual DOS Machine (VDM) process.

All DOS and 16-bit programs run on Windows 2000 in the Windows Virtual DOS Machine program. VDM simulates a 16-bit environment, complete with the DLLs required by 16-bit programs. By default, all 16-bit programs run as threads in a single, shared VDM process. As such, they share the memory space allocated to the VDM process and cannot run simultaneously.

Enabling this policy adds a check box to the Run dialog box, giving users the option of running a 16-bit program in its own dedicated NTVDM process. The additional check box is enabled only when a user enters a 16-bit program in the Run dialog box (Microsoft Developer's Network, 2000).

### ***Do not use the search based method when resolving shell shortcuts***

Prevents the system from conducting a comprehensive search of the target drive to resolve a shortcut.

By default, when the system cannot find the target file for a shortcut (.lnk), it searches all paths associated with the shortcut. If the target file is located on an NTFS partition, the system then uses the target's file ID to find a path. If the resulting path is not correct, it conducts a comprehensive search of the target drive in an attempt to find the file.

If you enable this policy, the system does not conduct the final drive search. It just displays a message explaining that the file is not found.

Note: This policy only applies to target files on NTFS partitions. FAT partitions do not have this ID tracking and search capability (Microsoft Developer's Network, 2000).

***Do not use the tracking based method when resolving shell shortcuts***

Prevents the system from using NTFS tracking features to resolve a shortcut.

By default, when the system cannot find the target file for a shortcut (.lnk), it searches all paths associated with the shortcut. If the target file is located on an NTFS partition, the system then uses the target's file ID to find a path. If the resulting path is not correct, it conducts a comprehensive search of the target drive in an attempt to find the file.

If you enable this policy, the system does not try to locate the file by using its file ID. It skips this step and begins a comprehensive search of the drive specified in the target path.

Note: This policy only applies to target files on NTFS partitions. FAT partitions do not have this ID tracking and search capability (Microsoft Developer's Network, 2000).

***Gray unavailable windows installer programs start menu shortcuts***

Displays Start menu shortcuts to partially installed programs in gray text.

This policy makes it easier for users to distinguish between programs that are fully installed and those that are only partially installed.

Partially installed programs include those that a system administrator assigns using Windows Installer and those that users have configured for full installation upon first use.

If you disable this policy or do not configure it, all Start menu shortcuts appear as black text.

Note: Enabling this policy can make the Start menu slow to open (Microsoft Developer's Network, 2000).

**Desktop**

***Hide all icons on Desktop***

Removes icons, shortcuts, and other default and user-defined items from the desktop, including Briefcase, Recycle Bin, My Computer, and My Network Places.

Removing icons and shortcuts does not prevent the user from using another method to start the programs or opening the items they represent (Microsoft Developer's Network, 2000).

***Remove my documents icon from desktop***

Removes most occurrences of the My Documents icon.

This policy removes the My Documents icon from the desktop, from Windows Explorer, from programs that use the Windows Explorer windows, and from the standard Open dialog box.

This policy does not prevent the user from using other methods to gain access to the contents of the My Documents folder.

This policy does not remove the My Documents icon from the Start Menu. To do so, use the "Remove My Documents icon from Start Menu" policy.

Note: To make changes to this policy effective, you must log off of and log back on to Windows 2000 (Microsoft Developer's Network, 2000).

***Remove my documents icon from start menu***

Removes the My Documents icon from the Start Menu and its submenus.

This policy only removes the icon. It does not prevent the user from using other methods to gain access to the contents of the My Documents folder.

Note: To make changes to this policy effective, you must log off of and log back on to Windows 2000 (Microsoft Developer's Network, 2000).

***Hide my network places icon on desktop***

Removes the My Network Places icon from the desktop.

This policy only affects the desktop icon. It does not prevent users from connecting to the network or browsing for shared computers on the network (Microsoft Developer's Network, 2000).

***Hide my Internet Explorer icon on desktop***

Removes the Internet Explorer icon from the desktop and from the Quick Launch bar on the taskbar.

This policy does not prevent the user from starting Internet Explorer by using other methods (Microsoft Developer's Network, 2000).

***Do not add shares of recently opened document to My network place***



Remote shared folders are not added to My Network Places whenever you open a document in the shared folder.

If you disable this policy or do not configure it, then when you open a document in a remote shared folder, the system adds a connection to the shared folder to My Network Places.

If you enable this policy, shared folders are not added to My Network Places automatically when you open a document in the shared folder (Microsoft Developer's Network, 2000).

### ***Prohibit users from changing My Documents path***

Prevents users from changing the path to the My Documents folder.

By default, a user can change the location of the My Documents folder by typing a new path in the Target box of the My Documents Properties dialog box. If you enable this policy, when users type a new path in the Target box, a message appears explaining that a policy prevents the action (Microsoft Developer's Network, 2000).

### ***Disable adding, dragging, dropping, and closing the taskbar's toolbar***

Prevents users from manipulating desktop toolbars.

If you enable this policy, users cannot add or remove toolbars from the desktop. Also, users cannot drag toolbars onto or off of docked toolbars.

Note: If users have added or removed toolbars, this policy prevents them from restoring the default configuration.

Tip: To view the toolbars that can be added to the desktop, right-click a docked toolbar (such as the taskbar beside the Start button), and point to "Toolbars" (Microsoft Developer's Network, 2000).

### ***Disable adjusting taskbar's toolbar***

Prevents users from adjusting the length of desktop toolbars. Also, users cannot reposition items or toolbars on docked toolbars.

This policy does not prevent users from adding or removing toolbars on the desktop.

Note: If users have adjusted their toolbars, this policy prevents them from restoring the default configuration (Microsoft Developer's Network, 2000).

### ***Don't save settings at exit***

Prevents users from saving certain changes to the desktop.

If you enable this policy, users can change the desktop, but some changes, such as the position of open windows or the size and position of the taskbar, are not saved when users log off.

However, shortcuts placed on the desktop are always saved (Microsoft Developer's Network, 2000).

### ***Active desktop***

#### ***Enable active desktop***

Enables Active Desktop and prevents users from disabling it.

This policy also removes the Active Desktop item from the context menu that appears when you right-click the desktop; it removes the Web tab from Display in Control Panel; and it disables the "Use Windows classic desktop" item on the General tab of the Folder Options dialog box. This prevents users from trying to enable or disable Active Desktop while a policy controls it.

If you disable this policy or do not configure it, Active Desktop is disabled by default, but users can enable it.

Note: If both the "Enable Active Desktop" policy and the "Disable Active Desktop" policy are enabled, the "Disable Active Desktop" policy is ignored. If the "Enable Classic Shell" policy (in User Configuration\Administrative Templates\Windows Components\Windows Explorer) is enabled, then Active Desktop is disabled and both of these policies are ignored.

Tip: To enable Active Desktop without setting a policy, right-click the desktop, point to "Active Desktop," and then click "Show Web Content" (Microsoft Developer's Network, 2000).

#### ***Disable active desktop***

Disables Active Desktop and prevents users from enabling it.

This policy also removes the Active Desktop item from the context menu that appears when you right-click the desktop; it removes the Web tab from Display in Control Panel; and it disables the "Enable Web content on my desktop" item on the General tab of the Folder Options dialog box. This prevents users from trying to enable or disable Active Desktop while a policy controls it. If you disable this policy or do not configure it, Active Desktop is disabled by default, but users can enable it.

Note: If both the "Enable Active Desktop" policy and the "Disable Active Desktop" policy are enabled, the "Disable Active Desktop" policy is ignored. If the "Enable Classic Shell" policy (in User Configuration\Administrative Templates\Windows Components\Windows Explorer) is

enabled, then Active Desktop is disabled and both of these policies are ignored.

Tip: To disable Active Desktop without setting a policy, right-click the desktop, point to "Active Desktop" and then turn off "Show Web Content" (Microsoft Developer's Network, 2000).

### ***Disable all items***

Removes Active Desktop content and prevents users from adding Active Desktop content.

This policy removes all Active Desktop items from the desktop. It also removes the Web tab from Display in Control Panel and removes the "New Desktop Item" command from the Active Desktop menu. As a result, users cannot add Web pages or pictures from the Internet or an intranet to the desktop.

This policy does not disable Active Desktop. Users can still use image formats, such as JPEG and GIF, for their desktop wallpaper (Microsoft Developer's Network, 2000).

### ***Prohibit changes***

Prevents the user from enabling or disabling Active Desktop or changing the Active Desktop configuration.

This is a comprehensive policy that locks down the configuration you establish by using other policies in this folder.

This policy removes the Web tab from Display in Control Panel and removes the Active Desktop item from menu that appears when you right-click the desktop. As a result, users cannot enable or disable Active Desktop. If Active Desktop is already enabled, users cannot add, remove, or edit Web content or disable, lock, or synchronize Active Desktop components (Microsoft Developer's Network, 2000).

### ***Prohibit adding items***

Prevents users from adding Web content to their Active Desktop.

This policy removes the "New" button from Web tab in Display in Control Panel. It also removes the "New Desktop Item" command from the Active Desktop menu. As a result, users cannot add Web pages or pictures from the Internet or an intranet to the desktop.

This policy does not remove existing Web content from their Active Desktop, or prevent users from removing existing Web content (Microsoft Developer's Network, 2000).

### ***Prohibit deleting items***

Prevents users from deleting Web content from their Active Desktop.

This policy removes the Delete button from the Web tab in Display in Control Panel. As a result, users can temporarily remove, but not delete, Web content from their Active Desktop.

This policy does not prevent users from adding Web content to their Active Desktop (Microsoft Developer's Network, 2000).

### ***Prohibit editing items***

Prevents users from changing the properties of Web content items on their Active Desktop.

This policy disables the Properties button on the Web tab in Display in Control Panel. Also, it removes the Properties item from the menu for each item on the Active Desktop. As a result, users can change the properties of an item, such as its synchronization schedule, password, or display characteristics (Microsoft Developer's Network, 2000).

### ***Prohibit closing items***

Prevents users from removing Web content from their Active Desktop.

In Active Desktop, you can add items to the desktop, but close them so they are not displayed. If you enable this policy, items added to the desktop cannot be closed; they always appear on the desktop.

This policy removes the list of the Active Desktop items from the Active Desktop menu. (To see this list, right-click the desktop and point to Active Desktop. The list appears at the bottom of the menu.) Also, it removes the check boxes from items on the Web tab in Display in Control Panel.

This policy does not prevent users from deleting items from their Active Desktop (Microsoft Developer's Network, 2000).

### ***Add/delete items***

Adds and deletes specified Web content items.

You can use the "Add" box in this policy to add particular Web-based items or shortcuts to users' desktops. Users can close or delete the items (if policies allow), but the items are added again each time the policy is refreshed.

You can also use this policy to delete particular Web-based items from users' desktops. Users can add the item again (if policies allow), but the item is deleted each time the policy is refreshed.

Note: Removing an item from the "Add" list for this policy is not the same as deleting it. Items removed from the add list are not removed from the desktop. They are just not added again (Microsoft Developer's Network, 2000).

### ***Active desktop wallpaper***

Specifies the desktop background ("wallpaper") displayed on all users' desktops.

This policy lets you specify the wallpaper on users' desktops and prevents users from changing the image or its presentation. The wallpaper you specify can be stored in a bitmap (\*.bmp), JPEG (\*.jpg), or HTML (\*.htm, \*.html) file.

To use this policy, type the fully-qualified path and name of the file that stores the wallpaper image. You can type a local path, such as C:\Winnt\Logo.bmp or a UNC path, such as \\Server\Share\Logo.bmp.

If the specified file is not available when the user logs on, no wallpaper is displayed. Users cannot specify alternate wallpaper.

You can also use this policy to specify that the wallpaper image be centered, tiled, or stretched. Users cannot change this specification.

If you disable this policy or do not configure it, no wallpaper is displayed. However, users can select the wallpaper of their choice.

Note: This policy requires that Active Desktop be enabled. By default, Active Desktop is disabled. To use a policy to enable Active Desktop, use the "Enable Active Desktop" policy (Microsoft Developer's Network, 2000).

### ***Allow only bitmapped wallpaper***

Permits only bitmap images for wallpaper.

This policy limits the desktop background ("wallpaper") to bitmap (.bmp) files. If users select files with other image formats, such as JPEG, GIF, PNG, or HTML, the wallpaper does not load.

This policy is designed to avoid the Active Desktop prompt. When users select a wallpaper with an alternate image format, the system prompts them to enable Active Desktop. By limiting users to bitmapped files, the prompt is avoided.

Also, see the "Active Desktop Wallpaper" and the "Disable changing wallpaper" (in User Configuration\Administrative Templates\Control Panel\Display) policies (Microsoft Developer's Network, 2000).

## ***Active directory***

### ***Maximum size of active directory searches***

Specifies the maximum number of objects the system displays in response to a command to browse or search Active Directory. This policy affects all browse displays associated with Active Directory, such as those in Local Users and Groups, Active Directory Users & Computers, and dialog boxes used to set permissions for user or group objects in Active Directory.

If you enable this policy, you can use the "Number of objects returned" box to limit returns from an Active Directory search.

If you disable this policy or do not configure it, the system displays up to 10,000 objects. This consumes approximately 2 MB of memory or disk space.

This policy is designed to protect the network and the domain controller from the effect of expansive searches (Microsoft Developer's Network, 2000).

### ***Enable filter to find dialog box***

Displays the filter bar above the results of an Active Directory search. The filter bar consists of buttons for applying additional filters to search results.

If you enable this policy, the filter bar appears when the Active Directory Find dialog box opens, but users can hide it.

If you disable this policy or do not configure it, the filter bar does not appear, but users can display it by selecting "Filter" from the "View" menu.

To see the filter bar, open My Network Places, click Entire Network, and then click Directory. Right-click the name of a Windows 2000 domain, and click Find. Type the name of an object in the directory, such as "Administrator." If the filter bar does not appear above the resulting display then, from the View menu, click Filter (Microsoft Developer's Network, 2000).

### ***Hide active directory folder***

Hides the Active Directory folder in My Network Places.

The Active Directory folder displays Active Directory objects in a browse window.

If you enable this policy, the Active Directory folder does not appear in the My Network Places folder.

If you disable this policy or do not configure it, the Active Directory folder appears in the My Network Places folder.

***This policy is designed to let users search Active Directory, but not tempt them to casually browse Active Directory (Microsoft Developer's Network, 2000).***

## Control panel

### ***Disable Control Panel***

Disables all Control Panel programs.

This policy prevents Control.exe, the program file for Control Panel, from starting. As a result, users cannot start Control Panel or run any Control Panel items.

This policy also removes Control Panel from the Start menu. (To open Control Panel, click Start, point to Settings, and then click Control Panel.) This policy also removes the Control Panel folder from Windows Explorer.

If users try to select a Control Panel item from the Properties item on a context menu, a message appears explaining that a policy prevents the action (Microsoft Developer's Network, 2000).

### ***Hide specified control panel applets***

Hides specified Control Panel items and folders.

This policy removes Control Panel items (such as Display) and folders (such as Fonts) from the Control Panel window and the Start menu. It can remove Control Panel items you have added to your system, as well Control Panel items included in Windows 2000.

To hide a Control Panel item, type the file name of the item, such as Ncpa.cpl (for Network). To hide a folder, type the folder name, such as Fonts.

This policy affects the Start menu and Control Panel window only. It does not prevent users from running Control Panel items.

Also, see the "Disable Display in Control Panel" policy in User Configuration\Administrative Templates\Control Panel\Display.

If both the "Hide specified control panel applets" policy and the "Show only specified control panel applets" policy are enabled, and the same item appears in both lists, the "Show only specified control panel applets" policy is ignored.

Tip: To find the file name of a Control Panel item, search for files with the .cpl file name extension in the %Systemroot%\System32 directory (Microsoft Developer's Network, 2000).

### ***Show only specified control panel applets***

Hides all Control Panel items and folders except those specified in this policy.

This policy removes all Control Panel items (such as Network) and folders (such as Fonts) from the Control Panel window and the Start menu. It removes Control Panel items you have added to your system, as well the Control Panel items

included in Windows 2000. The only items displayed in Control Panel are those you specify in this policy.

To display a Control Panel item, type the file name of the item, such as Ncpa.cpl (for Network). To display a folder, type the folder name, such as Fonts. If you do not specify any items or folders, the Control Panel window is empty.

This policy affects the Start menu and Control Panel window only. It does not prevent users from running any Control Panel items.

Also, see the "Disable Display in Control Panel" policy in User Configuration\Administrative Templates\Control Panel\Display.

If both the "Hide specified control panel applets" policy and the "Show only specified control panel applets" policy are enabled, the "Show only specified control panel applets" policy is ignored.

Tip: To find the file name of a Control Panel item, search for files with the .cpl file name extension in the %Systemroot%\System32 directory (Microsoft Developer's Network, 2000).

### ***Add/Remove programs***

#### ***Disable Add/Remove programs***

Prevents users from using Add/Remove Programs.

This policy removes Add/Remove Programs from Control Panel and removes the Add/Remove Programs item from menus.

Add/Remove Programs lets users install, uninstall, repair, add, and remove features and components of Windows 2000 and a wide variety of Windows programs. Programs published or assigned to the user appear in Add/Remove Programs.

If you disable this policy or do not configure it, Add/Remove Programs is available to all users.

When enabled, this policy takes precedence over the other policies in this folder.

This policy does not prevent users from using other tools and methods to install or uninstall programs (Microsoft Developer's Network, 2000).

#### ***Hide change or remove program page***

Removes the Change or Remove Programs button from the Add/Remove Programs bar. As a result, users cannot view or change the attached page.

The Change or Remove Programs button lets users uninstall, repair, add, or remove features of installed programs.



If you disable this policy or do not configure it, the Change or Remove Programs page is available to all users.

This policy does not prevent users from using other tools and methods to delete or uninstall programs (Microsoft Developer's Network, 2000).

#### ***Hide add new programs page***

Removes the Add New Programs button from the Add/Remove Programs bar. As a result, users cannot view or change the attached page.

The Add New Programs button lets users install programs published or assigned by a system administrator.

If you disable this policy or do not configure it, the Add New Programs button is available to all users.

This policy does not prevent users from using other tools and methods to install programs (Microsoft Developer's Network, 2000).

#### ***Hide add remove windows components page***

Removes the Add/Remove Windows Components button from the Add/Remove Programs bar. As a result, users cannot view or change the associated page.

The Add/Remove Windows Components button lets users configure installed services and use the Windows Component wizard to add, remove, and configure components of Windows 2000 from the installation files.

If you disable this policy or do not configure it, the Add/Remove Windows Components button is available to all users.

This policy does not prevent users from using other tools and methods to configure services or add or remove program components. However, this policy blocks user access to the Windows Component wizard (Microsoft Developer's Network, 2000).

#### ***Hide the "Add a program from CD-ROM or floppy disk" option***

Removes the Add a program from CD-ROM or floppy disk section from the Add New Programs page. This prevents users from using Add/Remove Programs to install programs from removable media.

If you disable this policy or do not configure it, the Add a program from CD-ROM or floppy disk option is available to all users.

This policy does not prevent users from using other tools and methods to add or remove program components.

Note: If the "Hide Add New Programs page" policy is enabled, this policy is ignored. Also, if the "Disable media source for any install" policy (located in Computer Configuration\Administrative Templates\Windows Components\Windows Installer) is enabled, users cannot add programs from removable media, regardless of the setting of this policy (Microsoft Developer's Network, 2000).

### ***Hide the "Add the program from Microsoft" option***

Removes the Add programs from Microsoft section from the Add New Programs page. This policy prevents users from using Add/Remove Programs to connect to Windows Update.

If you disable this policy or do not configure it, Add programs from Microsoft is available to all users.

This policy does not prevent users from using other tools and methods to connect to Windows Update.

Note: If the "Hide Add New Programs page" policy is enabled, this policy is ignored (Microsoft Developer's Network, 2000).

### ***Hide the "Add program from your network" option***

Prevents users from viewing or installing published programs.

This policy removes the Add programs from your network section from the Add New Programs page. The Add programs from your network section lists published programs and provides an easy way to install them.

Published programs are those that the system administrator has explicitly made available to the user with a tool such as Windows Installer. Typically, system administrators publish programs to notify users that the programs are available, to recommend their use, or to enable users to install them without having to search for installation files.

If you enable this policy, users cannot tell which programs have been published by the system administrator, and they cannot use Add/Remove Programs to install published programs. However, they can still install programs by using other methods, and they can view and install assigned (partially installed) programs that are offered on the desktop or on the Start menu.

If you disable this policy or do not configure it, Add programs from your network is available to all users.

Note: If the "Hide Add New Programs page" policy is enabled, this policy is ignored (Microsoft Developer's Network, 2000).

### ***Go directly to the components wizard***

Prevents users from using Add/Remove Programs to configure installed services.

This policy removes the Set up services section of the Add/Remove Windows Components page. The Set up services section lists system services that have not been configured and offers users easy access to the configuration tools.

If you disable this policy or do not configure it, Set up services appears only when there are unconfigured system services. If you enable this policy, Set up services never appears.

This policy does not prevent users from using other methods to configure services.

Note: When Set up services does not appear, clicking the Add/Remove Windows Components button starts the Windows Component wizard immediately. Because the only remaining option on the Add/Remove Windows Components page starts the wizard, that option is selected automatically, and the page is bypassed.

To remove Set up services and prevent the Windows Component wizard from starting, enable the "Hide Add/Remove Windows Components page" policy. If the "Hide Add/Remove Windows Components page" policy is enabled, this policy is ignored (Microsoft Developer's Network, 2000).

### ***Disable support information***

Removes links to the Support Info dialog box from programs on the Change or Remove Programs page.

Programs listed on the Change or Remove Programs page can include a "Click here for support information" hyperlink. When clicked, the hyperlink opens a dialog box that displays troubleshooting information, including a link to the installation files and data that users need to obtain product support, such as the Product ID and version number of the program. The dialog box also includes a hyperlink to support information on the Internet, such as the Microsoft Product Support Services Web page.

If you disable this policy or do not configure it, the Support Info hyperlink appears.

Note: Not all programs provide a support information hyperlink (Microsoft Developer's Network, 2000).

***Specify default category for Add new programs***

Specifies the category of programs that appears when users open the "Add New Programs" page.

If you enable this policy, then only the programs in the category you specify are displayed when the "Add New Programs" page opens. Users can use the Category box on the "Add New Programs" page to display programs in other categories.

To use this policy, type the name of a category in the Category box for this policy. You must enter a category that is already defined in Add/Remove Programs. To define a category, use Software Installation.

If you disable this policy or do not configure it, all programs (Category: All) are displayed when the "Add New Programs" page opens.

You can use this policy to direct users to the programs they are most likely to need.

Note: This policy is ignored if either the "Disable Add/Remove Programs" policy or the "Hide Add New Programs page" policy is enabled (Microsoft Developer's Network, 2000).

***Display***

***Disable display in control panel***

Disables Display in Control Panel.

If you enable this policy, Display in Control Panel does not run. When users try to start Display, a message appears explaining that a policy prevents the action (Microsoft Developer's Network, 2000).

***Hide background tab***

Removes the Background tab from Display in Control Panel.

This policy prevents users from using Control Panel to change the pattern and wallpaper on the desktop (Microsoft Developer's Network, 2000).

***Disable changing wallpaper***

Prevents users from adding or changing the background design of the desktop.

By default, users can use the Background tab of Display in Control Panel to add a background design (wallpaper) to their desktop. If you enable this policy, the

Background tab still appears, but all options on the tab are disabled.

To remove the Background tab, use the "Hide Background tab" policy.

To specify wallpaper for a group use the "Active Desktop Wallpaper" policy (Microsoft Developer's Network, 2000).

### ***Hide appearance tab***

Removes the Appearance tab from Display in Control Panel.

This policy prevents users from using Control Panel to change the colors or color scheme of the desktop and windows (Microsoft Developer's Network, 2000).

### ***Hide settings tab***

Removes the Settings tab from Display in Control Panel.

This policy prevents users from using Control Panel to add, configure, or change the display settings on the computer (Microsoft Developer's Network, 2000).

### ***Hide screen saver tab***

Removes the Screen Saver tab from Display in Control Panel.

This policy prevents users from using Control Panel to add, configure, or change the screen saver on the computer (Microsoft Developer's Network, 2000).

### ***No screen saver***

Disables all desktop screen savers.

If you enable this policy, screen savers do not run. Also, this policy disables the Screen Saver section of the Screen Saver tab in Display in Control Panel. As a result, users cannot change the screen saver options.

If you disable this policy or do not configure it, this policy has no effect on the system.

Note: This policy takes precedence over the "Screen saver executable name" policy. If both are enabled, the "Screen saver executable name" policy is ignored and no screen savers run (Microsoft Developer's Network, 2000).

### ***Screen saver executable name***

Specifies the screen saver for the user's desktop.

If you enable this policy, the system displays the specified screen saver on the user's desktop. Also, this policy disables the drop-down list of screen savers on the Screen Saver tab in Display in Control Panel, preventing users from changing the screen saver.

If you disable this policy, or do not configure it, users can select any screen saver.

To use this policy, type the name of the file that contains the screen saver, including the .scr file name extension. If the screen saver file is not in the %Systemroot%\System32 directory, enter the fully qualified path to the file.

If the specified screen saver is not installed on a computer to which this policy applies, the policy is ignored.

Note: This policy can be superceded by the "No screen saver" policy. If both are enabled, this policy is ignored and screen savers do not run (Microsoft Developer's Network, 2000).

### ***Password protect the screen saver***

Determines whether screen savers used on the computer are password protected.

If you enable this policy, all screen savers are password protected. If you disable this policy, password protection cannot be set on any screen saver.

This policy also disables the "Password protected" check box on the Screen Saver tab in Display in Control Panel, preventing users from changing the password protection setting.

If you do not configure this policy, users can choose whether or not to set password protection on each screen saver.

This policy is used only when a screen saver is specified for the computer. To specify a screen saver on a computer, in Control Panel, double-click Display, and then click the Screen Saver tab. To specify a screen saver in a policy, use the "Screen saver executable name" policy.

***Note: To remove the Screen Saver tab, use the "Hide Screen Saver tab"***

***policy (Microsoft Developer's Network, 2000).***

## ***Printers***

### ***Disable deletion of printers***

Prevents users from deleting local and network printers.

If a user tries to delete a printer, such as by using the Delete option in Printers in Control Panel, a message appears explaining that a policy prevents the action.

This policy does not prevent users from running other programs to delete a printer (Microsoft Developer's Network, 2000).

### ***Disable addition of printers***

Prevents users from using familiar methods to add local and network printers.

This policy removes the Add Printer option from the Start menu. (To find the Add Printer option, click Start, click Printers, and then click Add Printer.) This policy also removes Add Printer from the Printers folder in Control Panel.

Also, users cannot add printers by dragging a printer icon into the Printers folder. If they try, a message appears explaining that the a policy prevents the action.

However, this policy does not prevent users from using the Add Hardware wizard to add a printer. Nor does it prevent users from running other programs to add printers.

This policy does not delete printers that users have already added. However, if users have not added a printer when this policy is applied, they can't print.

Note: You can use printer permissions to restrict the use of printers without setting a policy. In the Printers folder, right-click a printer, click Properties, and then click the Security tab (Microsoft Developer's Network, 2000).

### ***Browse the network to find printers***

Lets users use the Add Printer wizard to search the network for shared printers.

If you enable this policy or do not configure it, then when users click "Add a network printer," but do not type the name of a particular printer, the Add Printer wizard displays a list of all shared printers on the network and invites users to choose a printer from among them.

If you disable this policy, users cannot search the network; they must type a printer name first.

This policy affects the Add Printer wizard only. It does not prevent users from using other programs to search for shared printers or to connect to network printers (Microsoft Developer's Network, 2000).

### ***Default active directory path when searching for printers***

Specifies the Active Directory location where searches for printers begin.

The Add Printer wizard gives users the option of searching Active Directory for a shared printer. If you enable this policy, these searches begin at the location you specify in the "Default Active Directory path" box. Otherwise, searches begin at the root of Active Directory.

This policy only provides a starting point for Active Directory searches for printers. It does not restrict user searches through the Active Directory (Microsoft Developer's Network, 2000).

### ***Browse a common web site to find printers***

Adds a link to an Internet or intranet Web page to the Add Printer wizard.

You can use this policy to direct users to a Web page from which they can install printers.

If you enable this policy and type an Internet or intranet address in the text box, the system adds a Browse button to the "Locate Your Printer" page in the Add Printer wizard. The Browse button appears beside the "Connect to a printer on the Internet or your intranet" option. When users click Browse, the system opens an Internet browser and navigates to the specified URL address to display the available printers.

This policy makes it easy for users to find the printers you want them to add (Microsoft Developer's Network, 2000).

## ***Regional options***

### ***Restrict selection of Windows 2000 menus and dialogs language***

This policy restricts users to the specified language, by disabling the menus and dialogs control in the Regional Options control panel. If the specified language is not installed on the target computer, the language selection will default to English (Microsoft Developer's Network, 2000).

## **Network**

### ***Offline files***

#### ***Disable user configuration of offline files***

Prevents users from enabling, disabling, or changing the configuration of Offline Files.

This policy removes the Offline Files tab from the Folder Options dialog box. It also removes the Settings item from the Offline Files context menu and disables the Settings button on the Offline Files Status dialog box. As a result, users cannot view or change the options on the Offline Files tab or Offline Files dialog box.

This is a comprehensive policy that locks down the configuration you establish by using other policies in this folder.

This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.



Tip: This policy provides a quick method for locking down the default settings for Offline Files. To accept the defaults, just enable this policy. You do not have to disable any other policies in this folder (Microsoft Developer's Network, 2000).

### ***Synchronize all offline files before logging off***

Determines whether offline files are fully synchronized when users log off.

This policy also disables the "Synchronize all offline files before logging off" option on the Offline Files tab. This prevents users from trying to change the option while a policy controls it.

If you enable this policy, offline files are fully synchronized. Full synchronization ensures that offline files are complete and current.

If you disable this policy, the system only performs a quick synchronization. Quick synchronization ensures that files are complete, but does not ensure that they are current.

If you do not configure this policy, the system performs a quick synchronization by default, but users can change this option.

This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Tip: To change the synchronization method without setting a policy, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then select the "Synchronize all offline files before logging off" option (Microsoft Developer's Network, 2000).

### ***Action of server disconnect***

Determines whether network files remain available if the computer is suddenly disconnected from the server hosting the files.

This policy also disables the "When a network connection is lost" option on the Offline Files tab. This prevents users from trying to change the option while a policy controls it.

If you enable this policy, you can use the "Action" box to specify how computers in the group respond.

-- "Work offline" indicates that the computer can use local copies of network files while the server is inaccessible.

-- "Never go offline" indicates that network files are not available while the server is inaccessible.

If you disable this policy or select the "Work offline" option, users can work offline if disconnected.

If you do not configure this policy, users can work offline by default, but they can change this option.

This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Tip: To configure this setting without establishing a policy, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, click Advanced, and then select an option in the "When a network connection is lost" section (Microsoft Developer's Network, 2000).

### ***Non-default server disconnect actions***

Determines how computers respond when they are disconnected from particular offline file servers. This policy overrides the default response, a user-specified response, and the response specified in the "Action on server disconnect" policy.

This policy also disables the "Exception list" section on the Offline Files tab. This prevents users from trying to change the option while a policy controls it.

To use this policy, click Show, and then click Add. In the "Type the name of the item to be added" box, type the server's computer name. Then, in the "Type the value of the item to be added" box, type "0" if users can work offline when they are disconnected from this server, or type "1" if they cannot.

This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Tip: To configure this setting without establishing a policy, in Windows Explorer, on the Tools menu, click Folder Options, click the Offline Files tab, and then click Advanced. This policy corresponds to the settings in the "Exception list" section (Microsoft Developer's Network, 2000).

### ***Disable "make available offline"***

Prevents users from making network files and folders available offline.

This policy removes the "Make Available Offline" option from the File menu and from all context menus in Windows Explorer. As a result, users cannot designate files to be saved on their computer for offline use.

However, this policy does not prevent the system from saving local copies of files that reside on network shares designated for automatic caching.

This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration (Microsoft Developer's Network, 2000).

### ***Disable use of offline files folder***

Disables the Offline Files folder.

This policy disables the "View Files" button on the Offline Files tab. As a result, users cannot use the Offline Files folder to view or open copies of network files stored on their computer. Also, they cannot use the folder to view characteristics of offline files, such as their server status, type, or location.

This policy does not prevent users from working offline or from saving local copies of files available offline. Also, it does not prevent them from using other programs, such as Windows Explorer, to view their offline files.

This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

***Tip: To view the Offline Files Folder, in Windows Explorer, on the Tools***

***menu, click Folder Options, click the Offline Files tab, and then click "View Files"***

***(Microsoft Developer's Network, 2000).***

### ***Administratively assign offline files***

Lists network files and folders that are always available for offline use. This policy makes the specified files and folders available offline to users of the computer.

To assign a folder, click Show and then click Add. In the "Type the name of the item to be added" box, type the fully qualified UNC path to the file or folder. Leave the "Enter the value of the item to be added" field blank.

Note: This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration (Microsoft Developer's Network, 2000).

### ***Disable reminder balloons***

Hides or displays reminder balloons, and prevents users from changing the setting.

Reminder balloons appear above the Offline Files icon in the status area to notify users when they have lost the connection to a networked file and are working on a local copy of the file. Users can then decide how to proceed.

If you enable this policy, the system hides the reminder balloons, and prevents users from displaying them.

If you disable the policy, the system displays the reminder balloons, and prevents users from hiding them.

If this policy is not configured, reminder balloons are displayed by default when you enable offline files, but users can change the setting.

To prevent users from changing the setting while a policy is in effect, the system disables the "Enable reminders" option on the Offline Files tab

This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

***Tip: To display or hide reminder balloons without establishing a policy, in Windows Explorer, on the Tools menu, click Folder Options, and then click the Offline Files tab. This policy corresponds to the "Enable reminders" check box (Microsoft Developer's Network, 2000).***

### ***Reminder balloon frequency***

Determines how often reminder balloon updates appear.

This policy also removes the "Display reminder balloon every ... minutes" option on the Offline Files tab. This prevents users from trying to change the option while a policy controls it.

Reminder balloons appear when the user's connection to a network file is lost or reconnected and are updated periodically. By default, the first reminder for an event is displayed for 30 seconds. Then, updates appear every 60 minutes and are displayed for 15 seconds. You can use this policy to change the update interval.

This policy appears in the Computer Configuration and User Configuration folders. if both policies are

configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Tip: To set reminder balloon frequency without establishing a policy, in Windows Explorer, on the Tools menu, click Folder Options, and then click the Offline Files tab. This policy corresponds to the "Display reminder balloons every ... minutes" option (Microsoft Developer's Network, 2000).

### ***Initial reminder balloon lifetime***

Determines how long the first reminder balloon for a network status change is displayed.

Reminder balloons appear when the user's connection to a network file is lost or reconnected and are updated periodically. By default, the first reminder for an event is displayed for 30 seconds. Then, updates appear every 60 minutes and are displayed for 15 seconds. You can use this policy to change the duration of the first reminder.

This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration (Microsoft Developer's Network, 2000).

### ***Reminder balloon lifetime***

Determines how long updated reminder balloons are displayed.

Reminder balloons appear when the user's connection to a network file is lost or reconnected and are updated periodically. By default, the first reminder for an event is displayed for 30 seconds. Then, updates appear every 60 minutes and are displayed for 15 seconds. You can use this policy to change the duration of the update reminder.

This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration (Microsoft Developer's Network, 2000).

### ***Event logging level***

Determines which events the Offline Files feature records in the event log.

Offline Files records events in the Application log in Event Viewer when it detects errors. By default, Offline Files records an event only when the offline files storage

cache is corrupted. However, you can use this policy to specify additional events you want Offline Files to record.

To use this policy, from the "Enter" box, select the number corresponding to the events you want the system to log. The levels are cumulative; that is, each level includes the events in all preceding levels.

"0" records an error when the offline storage cache is corrupted.

"1" also records an event when the server hosting the offline file is disconnected from the network.

"2" also records events when the local computer is connected and disconnected from the network.

"3" also records an event when the server hosting the offline file is reconnected to the network.

Note: This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration (Microsoft Developer's Network, 2000).

### ***Network and dialup connections***

#### ***Disable deletion of RAS connections***

Determines whether users can delete their private dial-up (RAS) connections.

If you enable this policy or do not configure it, users can delete their private RAS connections. Private connections are those that are available only to one user. (By default, only administrators can delete connections available to all users, but you can change the default by using the "Enable deletion of RAS connections available to all users" policy.)

If you disable this policy, users (including administrators) cannot delete any RAS connections. This setting also disables the "Delete" option on the context menu for a RAS connection and on the File menu in Network and Dial-up Connections.

Important: When disabled, this policy takes precedence over the "Enable deletion of RAS connections available to all users" policy. Users cannot delete any RAS connections and the "Enable deletion of RAS connections available to all users" policy is ignored.

Note: LAN connections are created and deleted automatically when a LAN adapter is installed or removed. You cannot use Network and Dial-up Connections to create or delete a local area connection.

Tip: To create a private connection, on the Connection Availability page in the Network Connections wizard, click the "Only for myself" option (Microsoft Developer's Network, 2000).

### ***Enable deletion of RAS connections available to all users***

Lets users delete shared dial-up (RAS) connections. Shared connections are available to all users of the computer.

If you enable this policy, users can delete shared RAS connections.

If you disable this policy or do not configure it, only administrators can delete shared RAS connections. (By default, users can still delete their private connections, but you can change the default by using the "Enable deletion of RAS connections" policy.)

Important: When disabled, the "Enable deletion of RAS connections" policy takes precedence over this policy. Users (including administrators) cannot delete any RAS connections and this policy is ignored.

Note: LAN connections are created and deleted automatically by the system when a LAN adapter is installed or removed. You cannot use Network and Dial-up Connections to create or delete a local area connection.

Tip: To create a shared RAS connection, on the Connection Availability page in the Network Connections wizard, click "For all users" (Microsoft Developer's Network, 2000).

### ***Enable connecting and disconnecting a RAS connection***

Determines whether users can connect and disconnect dial-up connections.

If you enable this policy, the Connect and Disconnect options for dial-up connections are available to users in the group. Users can connect or disconnect a dial-up connection by double-clicking the icon representing the connection, by right-clicking it, or by using the File menu.

If you disable this policy, then double-clicking the icon has no effect, and the Connect and Disconnect menu items are disabled.

Note: Users can still connect and disconnect from the Status page for a connection. To prevent users from displaying the Status page, disable the "Enable status statistics for an active connection" policy (Microsoft Developer's Network, 2000).

### ***Enable connecting and disconnecting a LAN connection***

Determines whether users can connect and disconnect local area connections.

If you enable this policy, the Connect and Disconnect options for local area connections are available to users in the group. Users can connect or disconnect a local area connection by double-clicking the icon representing the connection, by right-clicking it, or by using the File menu.

If you disable this policy, then double-clicking the icon has no effect, and the Connect and Disconnect menu items are disabled.

Note: Users can still connect and disconnect from the Status page for a connection. To prevent users from displaying the Status page, disable the "Enable status statistics for an active connection" policy (Microsoft Developer's Network, 2000).

### ***Enable access to properties of a LAN connection***

Determines whether users can view and change the properties of a local area connection.

This policy determines whether the Properties menu item is enabled, and thus, whether the Local Area Connection Properties dialog box is available to users.

If you enable this policy, a Properties menu item appears when users right-click the icon representing a local area connection. Also, when users select the connection, Properties is enabled on the File menu.

If you disable this policy, the Properties menu items are disabled, and users cannot open the Local Area Connection Properties dialog box.

Note: This policy supersedes policies that remove or disable parts of the Local Area Connection Properties dialog box, such as those that hide tabs, remove the check boxes for enabling or disabling components, or disable Properties button for components that a connection uses. If you disable this policy, then the policies that disable parts of the Local Area Connection Properties dialog box are ignored (Microsoft Developer's Network, 2000).

### ***Allow access to current user's RAS connection properties***

Determines whether users can view and change the properties of their private dial-up connections.



Private connections are those that are available only to one user. To create a private connection, on the Connection Availability page in the Network Connections wizard, click the "Only for myself" option.

This policy determines whether the Properties menu item is enabled, and thus, whether the Dial-up Connection Properties dialog box is available to users.

If you enable this policy, a Properties menu item appears when users right-click the icon representing a dial-up connection. Also, when users select the connection, Properties appears on the File menu.

If you disable this policy, the Properties menu items are disabled, and users cannot open the Dial-up Connection Properties dialog box.

Note: This policy supersedes policies that remove or disable parts of the Dial-up Connection Properties dialog box, such as those that hide tabs, remove the check boxes for enabling or disabling components, or disable the Properties button for components that a connection uses. If you disable this policy, it overrides these subsidiary policies (Microsoft Developer's Network, 2000).

### ***Enable access to properties of RAS connections available to all users***

Determines whether a user can view and change the properties of dial-up connections that are available to all users of the computer. To create such a connection, on the Connection Availability page in the Network Connections wizard, click the For all users option.

This policy determines whether the Properties menu item is enabled, and thus, whether the Dial-up Connection Properties dialog box is available to users.

If you enable this policy, a Properties menu item appears when users right-click the icon for a dial-up connection. Also, when users select the connection, Properties appears on the File menu.

If you disable this policy, the Properties menu items are disabled, and users cannot open the Dial-up Connection Properties dialog box.

Note: This policy supersedes policies that remove or disable parts of the Dial-up Connection Properties dialog box, such as those that hide tabs, remove the check boxes for enabling or disabling components, or disable the Properties button for components that a connection uses. If you disable this policy, it overrides these subsidiary policies.

Note: To find connections available to all users, see the Connections folder on your system drive (Documents

and Settings\All Users\Application Data\Microsoft\Network\Connections) (Microsoft Developer's Network, 2000).

***Enable renaming of connections, if supported***

Determines whether users can rename dial-up and local area connections.

If you enable this policy, the Rename option is enabled. Users can rename connections by clicking the icon representing a connection or by using the File menu.

If you disable this policy, the Rename option is disabled.

This policy is designed to be used with the "Enable renaming of RAS connections belonging to the current user" policy. When enabled, but not when disabled, the "Enable renaming of connections, if supported" policy takes precedence over the "Enable renaming of RAS connections belonging to the current user" policy.

The "Enable renaming of connections, if supported" policy permits users to rename all connections, including, but not limited to, their private dial-up connections. If the "Enable renaming of connections, if supported" policy is disabled and the "Enable renaming of RAS connections belonging to the current user" policy is enabled, users can rename only their private dial-up connections. However, if the "Enable renaming of connections, if supported" policy is enabled, then users can rename all connections, regardless of the setting of the "Enable renaming of RAS connections belonging to the current user" policy (Microsoft Developer's Network, 2000).

***Enable renaming of RAS connections belonging to the current user***

Determines whether users can rename their private dial-up connections.

Private connections are those that are available only to one user. To create a private connection, on the Connection Availability page in the Network Connections wizard, click the "Only for myself" option.

If you enable this policy, the Rename option is enabled for users' private dial-up connections. Users can rename their private connection by right-clicking an icon representing the connection or by using the File menu.

If you disable this policy, the Rename option is disabled, even on the user's private connections.

This policy is designed to be used with the "Enable renaming of connections, if supported" policy. When enabled (but not when disabled), the "Enable renaming of connections, if supported" policy takes precedence over this policy.

The "Enable renaming of connections, if supported" policy permits users to rename all connections, including, but not limited to, their private dial-up connections. If the "Enable renaming of connections, if supported" policy is disabled and the "Enable renaming of RAS connections belonging to the current user" policy is enabled, users can rename only their private dial-up connections. However, if the "Enable renaming of connections, if supported" policy is enabled, then users can rename all connections, regardless of the setting of the "Enable renaming of RAS connections belonging to the current user" policy (Microsoft Developer's Network, 2000).

### ***Enable adding and removing components for a RAS or a LAN connection***

Determines whether users can add and remove network components.

If you enable this policy, the Install and Uninstall buttons for components of connections in Network and Dial-up Connections are enabled. Also, users can gain access to network components in the Windows Components wizard.

If you disable this policy, the Install and Uninstall buttons for components of connections are disabled and users are not permitted access to network components in the Windows Components wizard.

The Install button opens the dialog boxes used to add network components. Clicking the Uninstall button removes the selected component in the components list (above the button).

The Install and Uninstall buttons appear when users right-click a connection and click Properties. These buttons are on the General tab for LAN connections and on the Networking tab for dial-up connections.

The Windows Components wizard permits users to add and remove components. To use the wizard, double-click Add/Remove Programs in Control Panel. To go directly to the network components in the Windows Components wizard, click the Advanced menu in Network and Dial-up Connections, and then click "Optional

Networking Components" (Microsoft Developer's Network, 2000).

***Allow connection components to be enabled or disabled***

Determines whether users can enable and disable the components used by dial-up and local area connections.

If you enable this policy, the Properties dialog box for a connection includes a check box beside the name of each component that the connection uses. Selecting the check box enables the component, and clearing the check box disables the component.

Disabling this policy removes the check boxes for enabling and disabling components. As a result, users cannot enable or disable the components that a connection uses (Microsoft Developer's Network, 2000).

***Enable access to properties of components of a LAN connection***

Determines whether users can change the properties of components used by a local area connection.

This policy determines whether the Properties button for components of a local area connection is enabled. If you enable this policy or do not configure it, the Properties button is enabled. If you disable this policy, the Properties button is disabled.

The Properties button opens the Local Area Connection Properties dialog box, which includes a list of the network components that the connection uses. To view or change the properties of a component, click the name of the component, and then click the Properties button beneath the component list.

Note: Not all network components have configurable properties. For components that are not configurable, the Properties button is always disabled (Microsoft Developer's Network, 2000).

***Enable access to properties of components of a RAS connection***

Determines whether users can view and change the properties of components used by a dial-up connection.

This policy determines whether the Properties button for components used by a RAS connection is enabled. If you enable this policy or do not configure it, the Properties button is enabled. If you disable this policy, the Properties button is disabled.

The Properties button opens the Dial-up Connection Properties dialog box, which includes a list of the network components that the connection uses. To view or change the properties of a component, click the name of the component, and then click the Properties button beneath the component list.

Note: Not all network components have configurable properties. For components that are not configurable, the Properties button is always disabled (Microsoft Developer's Network, 2000).

### ***Disable and enable the network connection wizard***

Determines whether users can use the Network Connection wizard, which creates new network connections.

If you enable this policy, the Make New Connection icon appears in Network and Dial-up Connections. Clicking Make New Connection starts the Network Connection wizard.

***If you disable this policy, the Make New Connection icon does not appear.***

***As a result, users cannot start the Network Connection wizard (Microsoft Developer's Network, 2000).***

### ***Enable status statistics for an active connection***

Determines whether users can view the Status page for an active connection.

The Status page displays information about the connection and its activity. It also provides buttons to disconnect and to configure the properties of the connection.

If you enable this policy, the Status page appears when users double-click an active connection. Also, an option to display the Status page appears on a menu when users right-click the icon for an active connection, and the option appears on the File menu when users select an active connection.

If you disable this policy, the Status option is disabled, and the Status page doesn't appear (Microsoft Developer's Network, 2000).

### ***Enable the dial-up preferences item on the advanced menu***

Determines whether the "Dial-up Preferences" item on the Advanced menu in Network and Dial-up Connections is enabled.

If you enable this policy, the Dial-up Preferences item is enabled. If you disable this policy, it is disabled. By default, Dial-up Preferences is enabled.

The Dial-up Preferences item lets users create and change connections before logon and configure automatic dialing and callback features (Microsoft Developer's Network, 2000).

### ***Enable the advanced settings item on the advanced menu***

Determines whether the Advanced Settings item on the Advanced menu in Network and Dial-up Connections is enabled.

If you enable this policy, the Advanced Settings item is enabled. If you disable this policy, it is disabled. By default, Advanced Settings is enabled.

The Advanced Settings item lets users view and change bindings and view and change the order in which the computer accesses connections, network providers, and print providers (Microsoft Developer's Network, 2000).

### ***Allow configuration of connection sharing***

Determines whether administrators can enable, disable, and configure the Internet Connection Sharing feature of a dial-up connection.

If you enable this policy or do not configure it, the system displays the Internet Connection Sharing (ICS) tab in the Properties dialog box for a dial-up connection. On Windows 2000 Server, it also displays the Internet Connection Sharing page in the Network Connection wizard. (This page is available only in Windows 2000 Server.)

If you disable this policy, the Internet Connection Sharing (ICS) tab and Internet Connection Sharing wizard page are removed.

Internet Connection Sharing lets users configure their system as an Internet gateway for a small network. It provides network services, such as name resolution, to the network.

By default, Internet Connection Sharing is disabled when you create a dial-up connection, but administrators can use the Internet Connection Sharing (ICS) tab and Internet Connection Sharing wizard page to enable it.

Note: This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Important: This policy applies only to users in the Administrators group (Microsoft Developer's Network, 2000).

### ***Allow TCP/IP advanced configuration***

Determines whether users can use Network and Dial-up Connections to configure TCP/IP, DNS, and WINS settings.

If you enable this policy, the Advanced button on the Internet Protocol (TCP/IP) Properties dialog box is enabled. As a result, users can open the Advanced TCP/IP Settings Properties page and modify IP settings, such as DNS and WINS server information.

If you disable this policy, the Advanced button is disabled and the users cannot open the Advanced TCP/IP Setting dialog box.

Note: If the "Enable access to properties of a LAN connection" policy or the "Enable access to properties of components of a LAN connection" policy are disabled, users cannot gain access to the Advanced button. As a result, this policy is ignored.

Tip: To open the Advanced TCP/IP Setting dialog box, in Network and Dial-up Connections, right-click a local area connection, and click Properties. In the "Components checked are used by this connection" box, click Internet Protocol (TCP/IP), click the Properties button, and then click the Advanced button (Microsoft Developer's Network, 2000).

## **System**

### ***Don't display welcome screen at logon***

Suppresses the "Getting Started with Windows 2000" welcome screen.

This policy hides the welcome screen that is displayed on Windows 2000 Professional each time the user logs on.

Users can still display the "Getting Started with Windows 2000" welcome screen by selecting it from the Start menu or by typing "Welcome" in the Run dialog box.

This policy applies only to Windows 2000 Professional. It does not affect the "Configure Your Server on a Windows 2000 Server" screen on Windows 2000 Server.

Note: This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Tip: To display the welcome screen, click Start, point to Programs, point to Accessories, point to System Tools, and then click "Getting Started." To suppress the welcome screen without setting a policy, clear the "Show this screen at startup" check box on the welcome screen (Microsoft Developer's Network, 2000).

### ***Century interpretation for year 2000***

Determines how programs interpret two-digit years.

This policy specifies the largest two-digit year interpreted as being preceded by 20. All numbers less than or equal to the specified value are interpreted as being preceded by 20. All numbers greater than the specified value are interpreted as being preceded by 19.

For example, the default value, 2029, specifies that all two-digit years less than or equal to 29 (00 to 29) are interpreted as being preceded by 20, that is 2000 to 2029. Conversely, all two-digit years greater than 29 (30 to 99) are interpreted as being preceded by 19, that is, 1930 to 1999.

This policy only affects the programs that use this Windows feature to interpret two-digit years. If a program does not interpret two-digit years correctly, consult the documentation or manufacturer of the program (Microsoft Developer's Network, 2000).

### ***Code signing for device drivers***

Determines how the system responds when a user tries to install device driver files that are not digitally signed.

This policy establishes the least secure response permitted on the systems of users in the group. Users can use System in Control Panel to select a more secure setting, but when this policy is enabled, the system does not implement any setting less secure than the one the policy established.

When you enable this policy, use the drop-down box to specify the desired response.

- "Ignore" directs the system to proceed with the installation even if it includes unsigned files.

- "Warn" notifies the user that files are not digitally signed and lets the user decide whether to stop or to proceed with the installation and whether to permit unsigned files to be installed. "Warn" is the default.

- "Block" directs the system to refuse to install unsigned files. As a result, the installation stops, and none of the files in the driver package is installed.



To change driver file security without setting a policy, use System in Control Panel. Right-click My Computer, click Properties, click the Hardware tab, and then click the Driver Signing button (Microsoft Developer's Network, 2000).

### ***Custom user interface***

Specifies an alternate user interface for Windows 2000.

The Explorer program (Explorer.exe) creates the familiar Windows interface, but you can use this policy to specify an alternate interface. If you enable this policy, the system start the interface you specify instead of Explorer.exe.

To use this policy, copy your interface program to a network share or to your system drive. Then, enable this policy, and type the name of the interface program, including the file name extension, in the Shell name text box. If the interface program file is not located in a folder specified in the Path environment variable for your system, enter the fully qualified path to the file.

If you disable this policy or do not configure it, the policy is ignored and the system displays the Explorer interface.

Tip: To find the folders indicated by the Path environment variable, click System Properties in Control Panel, click the Advanced tab, click the Environment Variables button, and then, in the System variables box, click Path (Microsoft Developer's Network, 2000).

### ***Disable the command prompt***

Prevents users from running the interactive command prompt, Cmd.exe. This policy also determines whether batch files (.cmd and .bat) can run on the computer.

If you enable this policy and the user tries to open a command window, the system displays a message explaining that a policy prevents the action.

Note: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Terminal Services (Microsoft Developer's Network, 2000).

### ***Disable registry editing tools***

Disables the Windows registry editors, Regedt32.exe and Regedit.exe.

If this policy is enabled and the user tries to start a registry editor, a message appears explaining that a policy prevents the action.

To prevent users from using other administrative tools, use the "Run only allowed Windows applications" policy (Microsoft Developer's Network, 2000).

### ***Run only allowed windows applications***

Limits the Windows programs that users have permission to run on the computer.

If you enable this policy, users can only run programs that you add to the List of Allowed Applications.

This policy only prevents users from running programs that are started by the Windows Explorer process. It does not prevent users from running programs such as Task Manager, which are started by the system process or by other processes. Also, if users have access to the command prompt, Cmd.exe, this policy does not prevent them from starting programs in the command window that they are not permitted to start by using Windows Explorer (Microsoft Developer's Network, 2000).

### ***Don't run specified windows applications***

Prevents Windows from running the programs you specify in this policy.

If you enable this policy, users cannot run programs that you add to the List of disallowed applications.

This policy only prevents users from running programs that are started by the Windows Explorer process. It does not prevent users from running programs, such as Task Manager, that are started by the system process or by other processes. Also, if you permit users to gain access to the command prompt, Cmd.exe, this policy does not prevent them from starting programs in the command window that they are not permitted to start by using Windows Explorer (Microsoft Developer's Network, 2000).

### ***Disable autoplay***

Disables the Autoplay feature.

Autoplay begins reading from a drive as soon as you insert media in the drive. As a result, the setup file of programs and the music on audio media starts immediately.

By default, Autoplay is disabled on removable drives, such as the floppy disk drive (but not the CD-ROM drive), and on network drives.

If you enable this policy, you can also disable Autoplay on CD-ROM drives, or disable Autoplay on all drives.

This policy disables Autoplay on additional types of drives. You cannot use this policy to enable Autoplay on drives on which it is disabled by default.

Note: This policy appears in both the Computer Configuration and User Configuration folders. If the settings conflict, the setting in Computer Configuration takes precedence over the setting in User Configuration (Microsoft Developer's Network, 2000).

### ***Download missing COM components***

Directs the system to search Active Directory for missing Component Object Model (COM) components that a program requires.

Many Windows programs, such as the MMC snap-ins, use the interfaces provided by the COM. These programs cannot perform all of their functions unless Windows 2000 has internally registered the required components.

If you enable this policy and a component registration is missing, the system searches for it in Active Directory and if it is found, downloads it. The resulting searches might make some programs start or run slowly.

If you disable this policy or do not configure it, the program continues without the registration. As a result, the program might not perform all of its functions, or it might stop.

This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration (Microsoft Developer's Network, 2000).

### ***Logon/Logoff***

#### ***Disable task manager***

Prevents users from starting Task Manager (Taskmgr.exe).

If this policy is enabled and users try to start Task Manager, a message appears explaining that a policy prevents the action.

Task Manager lets users start and stop programs; monitor the performance of their computers; view and monitor all programs running on their computers, including system services; find the executable names of programs; and change the priority of the process in which programs run (Microsoft Developer's Network, 2000).

#### ***Disable lock computer***

Prevents users from locking the system.

While locked, the desktop is hidden and the system cannot be used. Only the user who locked the system or the system administrator can unlock it.

Tip: To lock a computer without configuring a policy, press Ctrl+Alt+Delete, and then click "Lock Computer" (Microsoft Developer's Network, 2000).

#### ***Disable change password***

Prevents users from changing their Windows password on demand.

This policy disables the "Change Password" button on the Windows Security dialog box (which appears when you press Ctrl+Alt+Del).

However, users are still able to change their password when prompted by the system. The system prompts users for a new password when an administrator requires a new password or their password is expiring (Microsoft Developer's Network, 2000).

### ***Disable logoff***

Prevents the user from logging off of Windows 2000.

This policy does not let the user log off of the system by using any method, including programs run from the command line, such as scripts. It also disables or removes all menu items and buttons that log the user off of the system (Microsoft Developer's Network, 2000).

### ***Run logon scripts synchronously***

Directs the system to wait for the logon scripts to finish running before it starts the Windows Explorer interface program and creates the desktop.

If you enable this policy, Windows Explorer does not start until the logon scripts have finished running. This setting assures that logon script processing is complete before the user starts working, but it can delay the appearance of the desktop.

If you disable this policy or do not configure it, the logon scripts and Windows Explorer are not synchronized and can run simultaneously.

This policy appears in the Computer Configuration and User Configuration folders. The policy set in Computer Configuration takes precedence over the policy set in User Configuration (Microsoft Developer's Network, 2000).

### ***Run legacy logon scripts hidden***

Hides the instructions in logon scripts written for Windows NT 4.0 and earlier.

Logon scripts are batch files of instructions that run when the user logs on. By default, Windows 2000 displays the instructions in logon scripts written for Windows NT 4.0 and earlier in a command window as they run, although it does not display logon scripts written for Windows 2000.

If you enable this policy, Windows 2000 does not display logon scripts written for Windows NT 4.0 and earlier (Microsoft Developer's Network, 2000).

### ***Run logon scripts visible***

Displays the instructions in logon scripts as they run.

Logon scripts are batch files of instructions that run when the user logs on. By default, the system does not display the instructions in the logon script.

If you enable this policy, the system displays each instruction in the logon script as it runs. The instructions appear in a command window. This setting is designed for advanced users.

If you disable this policy or do not configure it, the instructions are suppressed (Microsoft Developer's Network, 2000).

### ***Run logoff scripts visible***

Displays the instructions in logoff scripts as they run.

Logoff scripts are batch files of instructions that run when the user logs off. By default, the system does not display the instructions in the logoff script.

If you enable this policy, the system displays each instruction in the logoff script as it runs. The instructions appear in a command window. This setting is designed for advanced users.

If you disable this policy or do not configure it, the instructions are suppressed (Microsoft Developer's Network, 2000).

### ***Connect home directory to root of the share***

Restores the definitions of the %HOMESHARE% and %HOMEPATH% environment variables to those used in Windows NT 4.0 and earlier.

If you enable this policy, the system uses the Windows NT 4.0 definitions. If you disable this policy or do not configure it, the system uses the new definitions designed for Windows 2000.

Along with %HOMEDRIVE%, these variables define the home directory of a user profile. The home directory is a persistent mapping of a drive letter on the local computer to a local or remote directory.

By default, in Windows 2000, %HOMESHARE% stores the fully qualified path to the home directory (such as \\server\share\dir1\dir2\homedir). Users can access the home directory and any of its subdirectories from the home drive letter, but they cannot see or access its parent directories. %HOMEPATH% stores a final backslash and is included for compatibility with earlier systems.

On Windows NT 4.0 and earlier, %HOMESHARE% stores only the network share (such as \\server\share). %HOMEPATH% stores the remainder of the fully qualified path to the home directory (such as \dir1\dir2\homedir). As a result, users can access any directory on the home share by using the home directory drive letter.

Tip: To specify a home directory in Windows 2000, in Active Directory Users and Computers or Local Users and Groups, right-click the name of a user account, click Properties, click the Profile tab, and in the "Home folder" section, select the "Connect" option and select a drive letter and home directory.

Example: Drive Z is mapped to \\server\share\dir1\dir2\homedir.

If this policy is disabled or not configured (Windows 2000 behavior):

```
-- %HOMEDRIVE% = Z: (mapped to
\\server\share\dir1\dir2\homedir)
-- %HOMESHARE% =
\\server\share\dir1\dir2\homedir
-- %HOMEPATH% = \
```

If the policy is enabled (Windows NT 4.0 behavior):

```
-- %HOMEDRIVE% = Z: (mapped to
\\server\share)
-- %HOMESHARE% = \\server\share
-- %HOMEPATH% = \dir1\dir2\homedir
```

(Microsoft Developer's Network, 2000).

### ***Limit profile size***

Sets the maximum size of each roaming user profile and determines the system's response when a roaming user profile reaches the maximum size.

If you disable this policy or do not configure it, the system does not limit the size of roaming user profiles.

If you enable this policy, you can do the following:

- Set a maximum permitted roaming profile size;
- Determine whether the registry files are included in the calculation of the profile size;
- Determine whether users are notified when the profile exceeds the permitted maximum size;
- Specify a customized message notifying users of the oversized profile;
- Determine how often the customized message is displayed.

(Microsoft Developer's Network, 2000).

### ***Exclude directories in roaming profile***

Lets you add to the list of folders excluded from the user's roaming profile.

This policy lets you exclude folders that are normally included in the user's profile. As a result, these folders need not be stored by the network server on which the profile resides, and do not follow users to other computers.

By default, the History, Local Settings, Temp, and Temporary Internet Files folders are excluded from the user's roaming profile.

If you enable this policy, you can exclude additional folders.

If you disable this policy or do not configure it, then only the default folders are excluded.

Note: You cannot use this policy to include the default folders in a roaming user profile (Microsoft Developer's Network, 2000).

### ***Run these programs at user logon***

Specifies additional programs or documents that Windows starts automatically when a user logs on to the system.

To use this policy, click Show, click Add and, in the text box, type the name of the executable program (.exe) file or document file. Unless the file is located in the %Systemroot% directory, you must specify the fully qualified path to the file.

Note: This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the system starts the programs specified in the Computer Configuration policy just before it starts the programs specified in the User Configuration policy (Microsoft Developer's Network, 2000).

### ***Disable the run once list***

Ignores customized run-once lists.

You can create a customized list of additional programs and documents that are started automatically the next time the system starts (but not thereafter). These programs are added to the standard list of programs and services that the system starts.

If you enable this policy, the system ignores the run-once list.

If you disable this policy, or do not configure it, the system runs the programs in the run-once list.

This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Tip: Customized run-once lists are stored in the registry in HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce (Microsoft Developer's Network, 2000).

### ***Disable legacy run list***

Ignores the customized run list for Windows NT 4.0 and earlier.

On Windows 2000 and Windows NT 4.0 and earlier, you can create a customized list of additional programs and documents that the system starts automatically when it starts. These programs are added to the standard run list of programs and services that the system starts.

If you disable this policy, or do not configure it, Windows 2000 adds any customized run list configured for Windows NT 4.0 and earlier to its run list.

If you enable this policy, the system ignores the run list for Windows NT 4.0 and earlier.

This policy appears in the Computer Configuration and User Configuration folders. If both policies are configured, the setting in Computer Configuration takes precedence over the setting in User Configuration.

Tip: To create a customized run list by using a policy, use the "Run these applications at startup" policy.

The customized run lists for Windows NT 4.0 and earlier are stored in the registry in HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run and HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Windows\Run. They can be configured by using the "Run" policy in System Policy Editor for Windows NT 4.0 and earlier (Microsoft Developer's Network, 2000).

## ***Group Policy***

### ***Group policy refresh interval for users***

Specifies how often Group Policy for users is updated while the computer is in use (in the background). This policy specifies a background update rate only for the Group Policies in the User Configuration folder.



In addition to background updates, Group Policy for users is always updated when they log on.

By default, user Group Policy is updated in the background every 90 minutes, with a random offset of 0 to 30 minutes.

You can specify an update rate from 0 to 64,800 minutes (45 days). If you select 0 minutes, the computer tries to update user Group Policy every 7 seconds. However, because updates might interfere with users' work and increase network traffic, very short update intervals are not appropriate for most installations.

If you disable this policy, user Group Policy is updated every 90 minutes (the default). To specify that Group Policy for users should never be updated while the computer is in use, select the "Disable background refresh of Group Policy" policy.

This policy also lets you specify how much the actual update interval varies. To prevent clients with the same update interval from requesting updates simultaneously, the system varies the update interval for each client by a random number of minutes. The number you type in the random time box sets the upper limit for the range of variance. For example, if you type 30 minutes, the system selects a variance of 0 to 30 minutes. Typing a large number establishes a broad range and makes it less likely that client requests overlap. However, updates might be delayed significantly.

Important: If the "Disable background refresh of Group Policy" policy is enabled, this policy is ignored.

Note: This policy establishes the update rate for user Group Policies. To set an update rate for computer Group Policies, use the "Group Policy refresh interval for computers" policy (located in Computer Configuration\Administrative Templates\System\Group Policy).

Tip: Consider notifying users that their policy is updated periodically so that they recognize the signs of a policy update. When Group Policy is updated, the Windows desktop is refreshed; it flickers briefly and closes open menus. Also, restrictions imposed by Group Policies, such as those that limit the programs a user can run, might interfere with tasks in progress (Microsoft Developer's Network, 2000).

### ***Group policy slow link detection***

Defines a slow connection for purposes of applying and updating Group Policy.

If the rate at which data is transferred from the domain controller providing a policy update to the computers in this group is slower than the rate specified by this policy, the system considers the connection to be slow.

The system's response to a slow policy connection varies among policies. The program implementing the policy can specify the response to a slow link. Also, the policy processing policies in this folder let you override the programs' specified responses to slow links.

To use this policy, in the "Connection speed" box, type a decimal number between 0 and 4,294,967,200 (0xFFFFFFFF), indicating a transfer rate in kilobits per second. Any connection slower than this rate is considered to be slow. If you type 0, all connections are considered to be fast.

If you disable this policy or do not configure it, the system uses the default value of 500 kilobits per second.

This policy appears in the Computer Configuration and User Configuration folders. The policy in Computer Configuration defines a slow link for policies in the Computer Configuration folder. The policy in User Configuration defines a slow link for policies in the User Configuration folder (Microsoft Developer's Network, 2000).

### ***Group policy domain controller selection***

Determines which domain controller the Group Policy snap-in uses.

-- "Use the Primary Domain Controller" indicates that the Group Policy snap-in reads and writes changes to the domain controller designated as the PDC Operations Master for the domain.

-- "Inherit from the Active Directory Snap-ins" indicates that the Group Policy snap-in reads and writes changes to the domain controller that Active Directory Users and Computers or Active Directory Sites and Services snap-ins use.

-- "Use any available domain controller" indicates that the Group Policy snap-in can read and write changes to any available domain controller.

If you disable this policy or do not configure it, the Group Policy snap-in uses the domain controller designated as the PDC Operations Master for the domain.

Tip: To change the PDC Operations Master for a domain, in Active Directory Users and Computers, right-click a domain, and then click "Operations Masters" (Microsoft Developer's Network, 2000).

### ***Create new group policy object links disable by default***

Creates new Group Policy object links in the disabled state.

This policy creates all new Group Policy object links in the disabled state by default. After you configure and test the new object links, either by using Active Directory Users and Computers or Active Directory Sites and Services, you can enable the object links for use on the system.

If you disable this policy or do not configure it, new Group Policy object links are created in the enabled state. If you don't want them to be effective until they are configured and tested, you must disable the object link. (Microsoft Developer's Network, 2000).

### ***Enforce show policies only***

Prevents administrators from viewing or using Group Policy preferences.

A Group Policy administration (.adm) file can contain both true policies and preferences. True policies, which are fully supported by Group Policy, must use registry entries in the Software\Policies or Software\Microsoft\Windows\CurrentVersion\Policies registry subkeys. Preferences, which are not fully supported, use registry entries in other subkeys.

If you enable this policy, the "Show Policies Only" command is turned on, and administrators cannot turn it off. As a result, Group Policy displays only true policies; preferences do not appear.

If you disable this policy or do not configure it, the "Show Policies Only" command is turned on by default, but administrators can view preferences by turning off the "Show Policies Only" command.

Tip: To find the "Show Policies Only" command, in Group Policy, click the Administrative Templates folder (either one), then right-click the same folder, and then point to "View."

In Group Policy, preferences have a red icon to distinguish them from true policies, which have a blue icon (Microsoft Developer's Network, 2000).

### ***Disable automatic update of ADM files***

Prevents the system from updating the Administrative Templates source files automatically when you open Group Policy.

By default, when you start Group Policy, the system loads the most recently revised copies of the Administrative Templates source files (.adm) that it finds in the %Systemroot%\inf directory. The .adm files create the list of policies that appear under Administrative Templates in Group Policy.

If you enable this policy, the system loads the .adm files you used the last time you ran Group Policy. Thereafter, you must update the .adm files manually.

Note: Upgrading your .adm files does not overwrite your policy configuration settings. The settings are stored in Active Directory, not in the .adm files.

Tip: To upgrade your .adm files manually, in Group Policy, right-click Administrative Templates (either instance), and then click Add/Remove Templates (Microsoft Developer's Network, 2000).

## INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center ..... 2  
8725 John J. Kingman Road, Suite 0944  
Ft. Belvoir, VA 22060-6218
  
2. Dudley Knox Library ..... 2  
Naval Postgraduate School  
411 Dyer Road  
Monterey, CA 93943-5101
  
3. Marine Corps Tactical Systems Support Activity ..... 1  
Technical Advisory Branch  
Attn: Librarian  
Box 555171  
Camp Pendleton, CA 92055-5080
  
4. Director, Marine Corps Research Center ..... 2  
MCCDC, Code C40RC  
2040 Broadway Street  
Quantico, VA 22134-5027
  
5. Director, Training and Education ..... 1  
MCCDC, Code C46  
1019 Elliot Road  
Quantico, VA 22134-5027
  
6. Paul C. Clark ..... 1  
Naval Postgraduate School  
clarkp@cs.nps.navy.mil
  
7. Cynthia Irvine ..... 1  
Naval Postgraduate School  
Irvine@cs.nps.navy.mil
  
8. Douglas E. Brinkley ..... 1  
Naval Postgraduate School  
dbrinkle@nps.navy.mil
  
9. William Haga ..... 1  
Naval Postgraduate School  
[haga@nps.navy.mil](mailto:haga@nps.navy.mil)

10.	Carl Siel.....	1
	Space and Naval Warfare Systems Command	
	sielc@sparwar.navy.mil	
11.	Elaine Cassara .....	1
	Branch Head, Information Assurance, USMC	
	CassaraES@hqmc.usmc.mil	
12.	Ms. Deborah M. Cooper.....	1
	Deborah M. Cooper Company	
	d.cooper@computer.org	
13.	Ms. Louise Davidson.....	1
	N643	
	davidson.louise@hq.navy.mil	
14.	Capt. James Newman .....	1
	N64	
	Newman.James@hq.navy.mil	
15.	Mr. Richard Hale.....	1
	Defense Information Systems Agency, Suite 400	
	<a href="mailto:haler@ncr.disa.mil">haler@ncr.disa.mil</a>	